The Rhetoric of Surveillance in Post-Snowden Background Investigation Policy Reform

by

Sarah Young

A Dissertation Presented in Partial Fulfillment
of the Requirements for the Degree
Doctor of Philosophy

Approved September 2016 by the
Graduate Supervisory Committee:

Peter Goggin, Chair
Shirley Rose
John Wise

ARIZONA STATE UNIVERSITY

May 2017

ABSTRACT

In June 2013, United States (US) government contractor Edward Snowden arranged for journalists at *The Guardian* to release classified information detailing US government surveillance programs. While this release caused the public to decry the scope and privacy concerns of these surveillance systems, Snowden's actions also caused the US Congress to critique how Snowden got a security clearance allowing him access to sensitive information in the first place. Using Snowden's actions as a kairotic moment, this study examined congressional policy documents through a qualitative content analysis to identify what Congress suggested could “fix” in the background investigation (BI) process. The study then looked at the same documents to problematize these “solutions” through the terministic screen of surveillance studies.

By doing this interdisciplinary rhetorical analysis, the study showed that while Congress encouraged more oversight, standardization, and monitoring for selected steps of the BI process, these suggestions are not neutral solutions without larger implications; they are value-laden choices which have consequences for matters of both national security and social justice. Further, this study illustrates the value of incorporating surveillance as framework in rhetoric, composition, and professional/technical communication research.

DEDICATION

Thank you to my closest alphabet of supporters: C, B, M, M, and my four legged cheerleaders M, B, and R. I'm both a long way and a short distance from being that wide-eyed kid from Kansas City, and I will never take for granted those that give and want nothing in return.

ACKNOWLEDGMENTS

My committee, Drs. Peter Goggin, Greg Wise, and Shirley Rose made this dissertation possible, and without their support, this project would still be an disassemblage of Word docs scattered about my computer. I give special thanks to my dissertation chair Peter Goggin for guiding the process and who was always upbeat no matter how many emails I sent his way.

TABLE OF CONTENTS

CHAPTER Page

APPENDIX Page

LIST OF TABLES

Table Page

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

In June 2013, government contractor Edward Snowden provided classified information to journalists at *The Guardian* so that they could publish details of the United States (US) government's surveillance programs. Three months later, government contractor Aaron Alexis murdered twelve people at the US Navy Yards in Washington, DC. While both incidents are very different, both shared the same commonality that each invovled a security clearance to access either sensitive data or a sensitive location. After these incidents, Congress recommended several suggestions to make the background investigation (BI) process better. While their suggestions to "fix" the process were along the lines of encouraging more surveillance, doing a rhetorical analysis of their recommendations through the terministic screen of surveillance studies problematizes what is considered a "solution."

One area of study largely overlooked in current rhetoric, composition, and also technical/ professional communication courses is surveillance. Attempts to locate English courses discussing surveillance through Google searches met with overwhelmingly negative results. While this didn't mean that these courses don't exist in English departments, the lack of immediate results shows that there is at least a probability that they are limited in number.[1] The searches involving English departments and surveillance that did appear were English department staff or students listing surveillance as a research interest (e.g., Beck, 2015; Crow, n.d.), but I could not locate substantial course work in writing studies devoted to surveillance. This is an unfortunate oversight though, as surveillance is a rich area full of promise with implications on all three areas of rhetoric, composition, and technical/professional communication.[2] Being watched causes certain behaviors, and just as the field can study sustainability and its related

[1] According to Google, Google Search reportedly provides results based on word choice and website authority so that most relevant responses are provided ("Algorithms," n.d.).

[2] I use the term technical and professional communication together based off of the work of Dobrin, Keller, and Weisser (2008) who define the phrase to mean "[c]ommunication about complex, highly detailed problems, issues, or subjects in the professional world, which helps audiences visualize and understand information so that they can make informed and ethical decisions or take appropriate or safe actions" (p .4).

influences, it can also study surveillance. Especially too, in an age increasingly dominated by technology where we might not realize we're being surveilled, it is important to have students rhetorically analyze spaces and places.

It was my objective then for my study to provide both an example which illustrated the value of investigating surveillance and incorporating surveillance into English departments and to use rhetoric to solve a research problem. In order to do this, I analyzed the discourse of Congressional documents discussing federal BIs since government contractor Edward Snowden divulged classified information in June 2013[3] to see what Congress suggested would be solutions to improving the BI process. I looked at this space because as a scholar and former background investigator, I was familiar with both the BI process as well as the ways in which rhetoric, composition, and professional and technical communication can be beneficial for analyzing BIs. I then looked at these same documents to see that despite one way of reading the documents suggested the recommendations were *solutions*, an alternative reading through surveillance shows how those same solutions could be *problems*.[4] In the final chapter of my dissertation, I look at the implications of the study results and show what these implications can mean for English departments.

Background on the Study

In June 2013, media installations such as *The Guardian* and *The Washington Post* began to publish classified United States (US) Government information provided to them by contractor Edward Snowden. This information detailed surveillance activity in the form of programs, collaborations, and databases that the US had been involved with both nationally and worldwide such as PRISM, Five Eyes, XKeyscore, and Enterprise Knowledge System.[5] Outcry resulted from

[3] I am interested in BIs after June 2013 for one specific reason, and that is because Congressional debate ensued after the government contractor Edward Snowden released highly classified information about the United States surveillance programs. This kairotic moment produced multiple documents advocating how to make the BI process better so that people like Snowden wouldn't gain access to sensitive information.

[4] This is especially interesting considering the word surveillance was only listed in the documents eighteen times, and it was never regarding the BI *as* surveillance (see appendix R).

the divulgence of this information, and since Snowden's revelations, there have been media debates in media outlets like the *New Yorker* and NPR over the limits of surveillance capabilities (Cassidy, 2013; "Debate," 2015). While the US justified these actions by saying surveillance was necessary for homeland and national security purposes (Campbell, 2013), many question the government's abilities to legally collect information such as telephone records, metadata, online data, and information about world leaders and ordinary Americans; the knowledge that mass surveillance was being conducted by the US government on all sorts of people beyond terrorists or enemies was a particularly concerning idea for some (Lyon, 2015).

This debate about privacy has been the most public debate on media channels, and while this is a worthy subject of consideration, it is not the only debate Snowden's actions have provoked and not the primary focus of this dissertation. While the idea of surveillance and privacy is part of this discussion, it did not drive the research questions. The primary endeavor for this dissertation, and another debate Snowden's disclosures ignited, was an examination of surveillance, security clearances, and BIs.

In order to have access to classified information, as Maryland Representative Elijah Cummings comments, individuals like Snowden must undergo BIs to minimize risk to national security (160 Cong., 2014). Once an individual passes their BI, they are considered vetted and trustworthy and are allowed access to specialized information (*The Navy Yard Tragedy*, 2013).

For the US Congress, due to the inability to stop Edward Snowden from divulging classified information, Snowden, a cleared government contractor, supposedly revealed that there were flaws in this BI process. According to congressional documents such as hearings and bills, because Snowden was allowed to get his clearance, there must be something wrong with the procedure.

[5] PRISM is a surveillance program designed to obtain communications from internet companies. Five Eyes is a surveillance collaboration between the US and Australia, Canada, New Zealand, the United Kingdom. XKeyscore is a computer system which assists in collecting internet information. According to Lucas (2014), the Enterprise Knowledge System is a series of related analytical and risk analysis databases which can group metadata.

As per Congress, a lack of ability to predict the future was not the cause of Snowden's disclosures; clearance processes had to have failed the American people. For example, Senator Rob Portman testified that Snowden's BI demonstrated "the inadequacies of the system" (*Safeguarding Our Nation's Secrets: Examining the Security Clearance Process*, 2013, p. 4), and because of unauthorized disclosures of information, Senator John Tester stated that "it is abundantly clear to the American people that the Federal Government is failing to properly vet the individuals who are granted access to our nation's most sensitive information and secure facilities" (*Safeguarding Our Nation's Secrets: Examining the National Security Workforce,* 2013, p. 1).

Snowden, however, is not the only catalyst in the conversation about BI reform. Three months after Snowden's disclosures started, in September 2013, civilian contractor Aaron Alexis entered the Washington Navy Yard and murdered twelve people before being fatally shot by police. Alexis was only able to access the property and facility where he committed these acts because he had a secret level clearance (*DC Navy Yard*, 2014). Had he not had this clearance, he could not have accessed the building where he carried out these murders. This incident, together with the Snowden incident three months earlier, caused the US House of Representatives and Senate to critically examine the BI process even further. Because of their actions, committees such as the House's Committee on Oversight and Government Reform (H.R.490, 2015) and Senate's Committee on Homeland Security and Governmental Affairs (S. 434, 2015) looked to reform the clearance process. As OPM's Inspector General (IG) Patrick McFarland summed up, "Recent events, including the horrific actions of Aaron Alexis and the unauthorized exposure of classified information by Edward Snowden show how critical it is to continuously improve and strengthen the background investigation process" (p. 18).

Rhetoric and BIs

One important thing to remember about this Congress' explanation however, is that this is not the only narrative that can be constructed around Snowden, Alexis, and BIs. Congress' deductions and any other conclusions made about Snowden, Alexis and BIs depend on how events are interpreted and terms are used. External truths don't exist outside of how

Congressional language constructs the events. Just as easily as IG McFarland advocated that the BI process should be strengthened, he could have also made the argument that no contractors whatsoever should have access to classified information. Both solutions could be argued to reduce the threat of disclosures of classified information, but McFarland did not advocate for the latter reason. Instead, like Senator Portman and Tester's comments, McFarland also advocated for a change to the BI process. McFarland thus chose a particular solution which supported one particular way of thought. In this sense then, Congress' interpretations were rhetorical. As opposed to a more philosophical view that looks at knowledge as absolute truth with language as a tool, rhetoric looks at knowledge as contingent and created through argument and persuasion rather than discovered and absolute (Bizzel & Herzberg, 1990). An external truth does not exist, and meaning is made only in the construction of arguments through language.

The purpose of this dissertation was to do a rhetorical analysis of Congressional documents from June 2013 to July 2015 to see what Congress argued needed to be fixed about BIs and further illustrate the value of incorporating studies of surveillance into rhetoric, composition, and technical/professional communication coursework. To meet this aim, specifically, this dissertation used the framework of Kenneth Burke's terministic screen. For Burke (1966/1990), terministic screens are lenses that we use to make sense of the world. According to Burke, "[M]uch that we take as observations about 'reality' may be but the spinning out of possibilities implicit in our particular choice of terms" (p. 1035). For Burke, the terministic screen is a specialized vocabulary which creates particular arguments to turn attention from one explanation of events to another. Congress essentially does this when they construct one version of the actions of Snowden and Alexis. To really see how the congressional documents only produced one account, I further analyzed the documents through terminology used in the field of surveillance studies which provided another specialized vocabulary through which to interpret the congressional communications.

Ultimately, I came to the conclusion that Congress' solution was advocating for more standardization with more types and more frequent evaluation to improve the BI process, but, by viewing these calls for more standardizations and monitoring through positions extolled through

surveillance studies, I concluded these recommendations are problematic and affect more than just an improved BI process.

Additionally, by using the theory of the terministic screen in my dissertation, I could also both look at what was present in the rhetoric used by Congress, and I could also see what was not present in their discussion, or as Burke (1984) says, “Every way of seeing is also a way of not seeing” (p. 70). I could see what was said and what was not said. In the case of my study, I concluded that the most overlooked stage of the BI process was the application step, and further, beyond this specific phase, the whole BI process is also taken for granted as the way to ensure safety and minimize risk. Supposedly, if a BI has been conducted, there is an assurance that adverse actions should be prevented, and any actions to the contrary equate to a poorly conducted BI rather than the inability to control the future.

The Study

This introduction lays the groundwork for my dissertation. While I was not necessarily interested in focusing on either Alexis or Snowden’s case in particular, I was interested in what Congress said caused and contributed to their security lapses for the BI. With this goal in mind, the main research question I set out to answer was: based on evidence from Congressional hearings, bills, daily editions, and reports, since Congress began to react to Snowden’s disclosures in June 2013, what arguments have emerged in the documents as flaws to the BI process? A secondary question to answer was: how does applying another terministic screen change the interpretation of the Congressional communication?

***Who* is involved?**

While Snowden and Alexis existed as stakeholders in the Congressional communication because Congress positioned them as catalysts for BI reform, for the purpose of my dissertation, the focus was not specifically on either person’s actions or statements. Although references to both occurred frequently in the discursive justifications for reform, for the purpose of this dissertation, the stakeholder involved in answering the primary research question was Congress (both the US House and Senate), and specifically the 113th and 114th sessions of Congress that were in session between June 2013 and July 2015. These sessions of Congress were in charge

of articulating both the problems and solutions for BIs through official record. By looking at the documents reviewed, I could see how leaders in these sessions defined the flaws of the BI process and defined what could be done to fix the flaws. The terms they used and arguments they constructed positioned BIs in certain ways that told a particular story, and analyzing these documents in particular helped construct the federal story of the BI in a post-Snowden environment.[6]

In addition to Snowden and Alexis, another stakeholder involved was the US Office of Personnel Management (OPM) and their Federal Investigative Service (FIS) division who, as of 2015, conducted ninety percent of the US government's background investigations for over one hundred federal agencies (USOPM, "Background Investigations," n.d.). Also, the lesser-publicized contractors for OPM who actually conducted seventy percent of OPM's investigations (*The Navy Yard Tragedy*, 2013) were integral to the conversation. One contractor of particular focus was US Investigation Services (USIS) who did the BI on both Snowden and Alexis (*The Insider Threat*, 2013). This agency declared bankruptcy in 2015, but it is often associated with the blame for the failure of the investigations (Wakeman, 2015) and decline in the whole BI process. For instance, in addition to skepticism about USIS after allegations of fraud, during a congressional hearing, Senator Tom Carper pointed out that USIS may have inadequately performed investigations of Alexis and Snowden, and this ultimately led to the question, "Are we at a crisis point with the credibility and integrity of the security clearance process? What should give us any faith in the current system?" (*The Navy Yard Tragedy*, 2013, p. 18).

Another government agency, the Government Accountability Office (GAO), is also a stakeholder in the congressional documents analyzed in this dissertation; many of the reports involved in this study were published by the GAO (USGAO, 2013; 2014a; 2014b) or had testimony from Brenda Farrell, the Director, Defense Capabilities and Management, Military and

[6] As seen by leading surveillance theorist David Lyon (2015), Snowden's actions were monumental enough to create a differentiation between a pre and post era. Even the director of the FBI refers to 2014 as "post-Snowden" (Comey, 2014). While this idea can be contested and deserves its own conversation, it will not be explored further in this dissertation, see Lyon (2015) and Margulies (2015) for further discussion.

Department of Defense (DOD) Civilian Personnel Issues at the GAO (*DC Navy Yard Shooting*, 2014; *The Insider Threat to Homeland Security*, 2013; *The Navy Yard Tragedy*, 2013; *Safeguarding Our Nation's Secrets: Examining the Security Clearance Process*, 2013; *Safeguarding Our Nation's Secrets: Examining the National Security Workforce*, 2013).

What **is Being Studied?**

Again, while Alexis and Snowden were the catalysts for this discussion, they were not the primary focus of study for this dissertation. As the first research question addressed the recommendations for BI reform, the main focus of the study was examining what needed to be fixed in the BI process. As the secondary question addressed the differences between conclusions when an alternative terministic screen was applied, a second focus of this dissertation was applying a separate terministic screen to the data so that the congressional documents could be interpreted with a separate lens; in this case, that lens was the field of surveillance studies.

Also central to this dissertation was the main unit of this study – the BI. For more on BIs themselves, as will be discussed further in chapter two, BIs are essentially ways that the US government monitors and controls (potential) employees and individuals that wish to have access to certain federal resources. For a quick definition, according to Congress, and specifically, the US Senate, a BI is:

> any investigation required for determining the eligibility of a covered individual for logical and physical access to federally controlled facilities or information systems; suitability or fitness of a covered individual for federal employment; eligibility of a covered individual for access to classified information or to hold a national security sensitive position; or fitness of a covered individual to perform work on or behalf of the United States Government as a contractor employee. (S. 113-276, 2014)

These investigations supposedly identify potential lifestyle habits or personality traits that may indicate future problematic behavior such as holding a passport to a foreign country or inability or refusal to pay debts (USDOS, 2006). To identify potential risks, BIs use surveillance to assemble information which purportedly combines to create a whole picture of a subject of investigation.

This whole person[7] is subsequently compared to agency standards to see if the applicant meets expectations of the position.

BIs then essentially surveil employees in order to vet them for these specific positions and access. In Snowden and Alexis' case, in the above definition, both of their BIs concerned the "eligibility of a covered individual for access to classified information or to hold a national security sensitive position" (S. 113-276, 2014), so for the most part, *national security* BIs were the main consideration for this dissertation.

***Where* information0Ccomes From**

What this dissertation studied was BI reform, and *where* this information came from was Congressional documents. I turned to Congressional documents because these types of documents are the primary sources of information distributed by Congress that would discuss BI reform. I wanted to study these institutions because they are the legislative branch of government, so they are responsible for examining and forming BI regulation.

In order to select those documents, I used the Arizona State University library search tool *One Search* and the Boolean search phrase "(U.S. Congress) AND ("background investigations") AND ("security clearance process")." I selected those keywords because my main objective was to see what Congress had to say BIs for security clearances since this was the main topic of discussion after Snowden and Alexis. The results of the search were twenty-nine documents which came in four formats: hearings, bills, acts, and congressional records. The contents of these documents reflected a range of purposes from more argumentative debates during hearings to the more solidified actions for bills and acts. Of note, in the document search, two of the documents were repeats and four articles could not be accessed. Because of this, these documents were omitted. Thus, overall, the study was based on twenty-three documents. In total, this was approximately 1,579 pages of text. A more detailed discussion of articles and methods

[7] Congress positions the "whole person" concept as the basis of adjudication. According to the US House of Representatives, this means that an individual is evaluated based on "a careful weighing of available, reliable information about the person, past and present, favorable and unfavorable" (*The Insider Threat*, 2013, p. 15). This construct forms the foundation of the BI and lends credibility to it by reinforcing the idea that BIs supposedly can, in fact, capture a reliable and entire essence of an applicant (Young, forthcoming).

will be discussed in chapter three. Other journalistic and scholarly pieces were used fill in gaps between documents to understand how Congress was forming their argument, but these secondary pieces were used to make sense of the study's results and were not part of the study itself.

When Was information Gathered?

After entering these search terms, I selected only "government" documents published from June 2013 to July 2015 (time of data gathering) in order to limit the documents to material published by the US government since Snowden began divulging information. I did this because I was interested in Congress' reforms in a post-Snowden/Alexis environment. This compilation of documents worked best for my study because after doing a cursory analysis of the documents, they offered a fundamental discussion of what background investigations are, what current problems were, and what suggested solutions should be. While it would be good to compare my selected time period to other time spans such as the more recent period before Snowden around the WikiLeaks or Bradley Manning incidents, further back to the period after another famous security leak of Aldrich Ames in the mid-1990s, or even the origin of BIs themselves after Executive Order (EO) 10450 in 1953 (*Safeguarding Our Nation's Secrets: Examining the National Security Workforce*, 2013), this would be more suited to a larger study and beyond the scope of this investigation. As stated, this dissertation's focus was on the calls for BI reform in a post-Snowden environment.

Why Should the Study Be Conducted?

This topic should be studied because a scholarly examination of BIs has not been done. In fact, BIs in academic contexts are often overlooked in areas outside of justice studies or business, and if BIs are examined, the discussions typically treat BIs as assumptions of fact without much question or criticism. For instance, peer reviewed literature from justice studies and business (Ferraro & Spain, 2006; McDaniel, Lees, & Wynn, 1995; Ritch, 1997; Slora, Joy, Jones, & Terris, 1991) operate under the assumption that in order to vet someone as trustworthy, just conduct a thorough BI to prevent future problems. Recommendations about BIs are often procedural and structured around best practices, (Ferraro & Spain, 2006; Ritch, 1997) or highlight

ways to conduct BIs to avoid retaliatory litigation (Ferraro & Spain, 2006; Ritch, 1997). There are some resources that complicate the idea of BIs by tackling related topics such as the validity of the BI's prediction of on-the-job violence (Slora, Joy, Jones, & Terris, 1991) or use of credit reports when screening for future employees (McDaniel, Lees, & Wynn, 1995), but a more direct review of the BIs is lacking. Overwhelmingly, the concept of the BI is left unchallenged. In order to have confidence in personnel, just conduct a BI and organizations will be safe.

As this dissertation shows though, an examination of the congressional assumptions about the clearance process complicates the overall faith institutions put in BIs. BIs for clearances weren't taken as just facts or procedures, and the BI was presented as an arguable piece of rhetoric. Further, the congressional solutions were also examined as pieces of argument, constructed in certain ways that both defined what the problems were while simultaneously defining what the problems were not. As Kenneth Burke (1945) points out, vocabularies are built on what is presumed to be "faithful *reflections* of reality" but these vocabularies are really just "*selections* of reality" and thus merely function as a "*deflection* of reality" (p. 59). In other words, when developing arguments, the reasons given are only based on a reduction of reality, but there are other possible readings and possibilities for any explanations given. As in the case of Congress, the overt reasons Congress provided for the need for background investigation reform are just one way to look at the issue, and Congress was only constructing one side of the story.

Importantly, this complication of underlying assumptions about the BI has implications beyond the context of security clearances as BIs are often used in many other situations to vet individuals. First, this can be seen in events such as the reaction to the relocation of Syrian refugees in the United States after the ISIS bombings in Paris. After the attacks on November 13, 2015, some in Congress such as Representative Michael McCaul from Texas and Representative Richard Hudson from North Carolina proposed and passed a bill halting refugee relocation until more thorough BIs were conducted to ensure refugees were thoroughly vetted (H.R. 4038, 2015; Kelly, 2015a). This bill, H.R. 4038: American SAFE Act of 2015, was introduced to the US House of Representatives on November 17, 2015 and passed with urgency two days later, expanding background checks on Iraqi and Syrian refugees (H.R. 4038). In this case, BIs are treated like *the*

way to ensure no refugees are terrorists. More and more thorough BIs are the way to mitigate risks. This dissertation though shows that assuming the infallibility of BIs is a problematic move.

Additionally, BIs are also taken for granted in instances like gun purchasing (H.R. 1025, 1993) and residential applications ("Tenant Screening," n.d.). For instance, H.R. 1025 (or the "Brady Bill") assumes that if an individual passes a BI, they should be trusted with a firearm (H.R. 1025, 1993), and according to Criminal History Checks, BIs for residential applications assumes that if a prospective tenant passes the check, they will be a good lessee that pays bills on time and will ensure a community's safety ("Tenant Screening," n.d.). Both examples are also troubling if one considers the problematic nature of believing a BI can predict the future. While all three of these illustrations are not discussed within the scope of this dissertation, they do provide evidence that this discussion of the BI has merit and is worthy of discussion for not just security clearances but for other community issues.

How **Was the Study Conducted?**

For my dissertation, I used qualitative content analysis. A content analysis involves "describing the meaning of qualitative data (Schreier, 2014, p. 170)" and "is done by assigning successive parts of the material to the categories of a coding frame." In the case of this dissertation, the main frames were the articulated problems and solutions of BIs. The initial categorizing generated over one hundred 12x12 pages of data arranged into three subcategorizes. Chapter three breaks this down further, but briefly, the first frame was "current mistrust" which was grounded by congressional passages reflecting the belief that BIs may not be doing what they are supposed to do due to current BI practices. This section discussed both the problems and solutions for BIs. The second frame was a "fundament mistrust" of BIs which was based on the idea that BI principals and assumptions are fundamentally flawed or not as safe as it seems overall. This section features statements that acknowledge the fallibility of BIs.[8] The third frame was "trust" and grouped together passages were BIs were argued to be a trusted part of vetting procedures. Each of these frames provided rough data for the primary research question.

[8] This was the shortest section of the results and was less than two full pages.

The content of the data will be discussed in greater detail in chapter four when the study is explained.

In order to view Congress' discussion about BIs as only one terministic screen, the results were analyzed through the lens of surveillance studies to provide a richer analysis. I used the field of surveillance studies because this field is concerned with issues of monitoring and national security. In order to incorporate this lens, I organized and coded the documents under review into eight areas commonly discussed in surveillance studies literature: constancy, surveillant assemblage, surveillers, sorting, risk, prediction, identity, and technology.

Roadmap

As stated, the questions I set out to answer were: based on Congressional hearings, bills, daily editions and reports, since Congress began to react to Snowden's disclosures in June 2013, what arguments have emerged in the documents as flaws to the BI process? And how does applying another terministic screen change the interpretation of the Congressional communication? In order to answer these questions, this dissertation was arranged in the following order. Chapter one, this introduction, lays out an overview of the dissertation. Chapter two is a literature review for rhetoric, surveillance, and BIs. This chapter looks at the terministic screen, explores the eight themes of surveillance studies, and briefly details the fundamentals of BIs. The third chapter discusses the methodology of the study and outlines qualitative content analysis. The fourth chapter describes how I made meaning from interpreting the results of this study. The fifth chapter discusses the implications and significance of the study's results.

Additional pertinent information

This discussion of BIs is of special interest to me due to my employment experience for almost twelve years as a background investigator. From 2002 to 2014, I was involved in conducting fieldwork for BIs. In response to the events of September 11th, 2001, requests for background investigations skyrocketed, and in April 2002, I was tentatively hired to help control the backlog as an intern for OPM's only contractor at the time, USIS. Four months later in August 2002 after my own background investigation cleared, I started working for the agency as an intern and record searcher. I became a full investigator the following summer, and I worked diligently for

the company as a senior investigator until February 2014 when the agency began to unravel. In charge of doing both Snowden and Alexis' background check, Congress suggested that the agency had conducted faulty investigations, and the agency's work became highly scrutinized (*The Navy Yard Tragedy*, 2013). According to Congress as will be discussed in chapter four, better investigative processes could have prevented their security lapses.

Six months after leaving USIS, the problems that had been brewing when I left in February culminated in the dissolution of my former agency. In addition to the beliefs in the failure of Snowden and Alexis' BIs, coupled with allegations of mismanagement and fraud, and after a cyber-attack from an international source on USIS' OPM computer system (Kelly, 2015b), in August 2014, all USIS investigative staff was put on a terminal furlough. OPM let their contract with USIS end, and the company's investigator service division dissolved. Although I had already left, it was not a choice I had wanted to make; I liked working with a sense of civic purpose. But after giving USIS almost twelve years, hours of overtime, and almost all of my 20's under the watch of metrics and deadlines, the company ended in bankruptcy, disgraced and discredited, and I was left wondering how a company, full of people that cared so much about meeting all the handbook criteria for accurate and complete BIs, could have either let Snowden or Alexis "slip through the cracks" or could be blamed for not predicting the future. Either way, I was left in conflict over the fundamental principles of BIs. I genuinely wanted to know how Congress defined and described the problems and solutions for reform. How could these slips have been prevented? Could they have been?

So in addition to the applied and academic motivations, I also had a personal desire to research BIs for almost therapeutic reasons, to make sense of the mess of the situation. There had to be significance in this, and I was in a position to join my understanding of the industry, use of rhetorical analysis, and theoretical framework of surveillance into a larger project of meaning-making. This dissertation attempted to reconcile both my academic and personal interest in this area of study and come to terms with what a BI is, what it supposedly can do, what faith that we put in this system of vetting, and how this area can exemplify the value for incorporating studies of surveillance into English departments.

CHAPTER 2

LITERATURE REVIEW

Because this dissertation straddled two areas of study – both rhetoric and surveillance studies, this chapter offers an overview of both concepts (e.g., such as a history or rhetoric) so that readers unfamiliar with either discipline may be able to understand both elements of the framework more thoroughly. Further, in order to situate my analysis of congressional records into the discourse of surveillance studies, I use this chapter in two key ways. First I discuss rhetoric and the terministic screen to show how surveillance studies functioned in this dissertation. Second, I discuss principles of surveillance to set the foundation for chapter four which explicitly shows how BIs are in fact acts of surveillance. Seeing BIs as surveillance helps problematize the responses to question one. I also offer a brief explanation of Federal BIs to explain what a federal BI for a security clearance entails so that the reader is able to understand the process of the BI and the terms that are used when describing it throughout the rest of the dissertation. However, I did not consider this third section part of this chapter's primary aim.

Rhetoric - The Art of Seeing What Isn't There

As a reminder, the primary research question asks: based on congressional hearings, bills, daily editions, and reports, since Congress began to react to Snowden's disclosures in June 2013, what arguments have emerged in the documents as flaws to the BI process? This question is essentially asking what argument did Congress construct to address the BI process after Snowden, or another way to put it, what is Congress' post-Snowden BI rhetoric? As stated in chapter one, rhetoric looks at knowledge as contingent and created through argument and persuasion rather than discovered and absolute (Bizzel & Herzberg, 1990), so in these respects then, an understanding of the term rhetoric is essential to understanding what it means when I say there are other ways to construct an argument.

Further, the second question asks, how does applying another terministic screen change the interpretation of the congressional communication? It is thus essential to understand Burke's rhetorical theory of the terministic screen to see that although Congress position BIs as failing in

certain ways with particular ways to fix these failings, this is just one explanation of the events that transpired.

History of Rhetoric

Rhetoric is often traced back to the fifth century B.C.E. to Greek probate courts where it was important to understand the art of persuasion (Bizzell & Herzberg, 1990). In order to convince others and win disputes, citizens needed well-constructed arguments that were convincing both logically and emotionally. Some orators began teaching strategies for organizing and delivering speeches, and this activity became known as rhetoric. Consequently, according to Bizzell and Herzberg (1990), "*Rhetoric* thus came to designate both the practice of persuasive oratory and the description of ways to construct a successful speech" (p. 2). People thus used rhetoric as a tactic to convince and persuade others.

Today, this classical understanding of rhetoric persists. According to Blakesley (2012), often, "the term *rhetoric* has been used to name either (1) the use of persuasive resources (*rhetorica utens*), or (2) the *study* of the use of persuasive resources (*rhetorica docens*)" (p. 14), and we generally think of rhetoric as a performance where one works to convince the audience. A popular definition of rhetoric often evoked in the composition classroom is Aristotle's notion that rhetoric "is the faculty of observing in any given case the available means of persuasion" (Aristotle, 1990, p. 153). Rhetoric is thus still understood to mean finding ways to appeal to the desires of others for persuasive reasons. In order to teach this principle, Aristotle's three appeals of ethos, pathos, and logos in the form of the rhetorical triangle are often discussed as techniques of persuading an audience, especially in freshman composition textbooks (e.g., Clark, 2012; Lunsford, Ruszkiewicz, & Walters, 2013; Seyler, 2012). A common first year composition activity involves students conducting a version of rhetorical analysis by identifying these appeals in any given text to point out when arguments appeal to character, emotion, or logic. In these respects, rhetoric thus often stays classically linked with recognizing techniques used to convince others of one's position; appeals such as ethos, pathos, and logos become heuristics to breakdown and classify arguments.

Not all rhetorical study is just concerned with the ancient Greek's idea of techniques of identifying and constructing arguments for optimum persuasion though. Blakesley (2012) continues that rhetoric also studies "*how* and *why* people use persuasion in the first place" (p. 14). Bizzel & Herzberg (1990) agree and add that this more philosophical view has emerged more recently when many twentieth century rhetoricians have expanded the scope of rhetoric so that rhetoric has overall become "a comprehensive theory of language and effective discourse" (p. 899) beyond just a taxonomy through appeals. This expanded understanding of rhetoric includes discussions of social behavior and how power and ideology are expressed through communication.

Analyzing power and ideology is important to do because looking at behaviors and identifying the ideology behind arguments helps break down what a population may assume is fact or believe through consensus (Blakesley, 2012).[9] To clarify, some of society's arguments are repeated throughout time and place and the origin of logic of the argument is not thoroughly examined. For instance, sociologist Deborah Lupton (1999) points out that pregnant women are often drawn into the narrative that an unborn baby is fragile and any problems with a fetus is the mother's fault. This narrative is not necessarily true, but societies such as the United States tend to subscribe to this belief. Similarly, for the BI, Congress constructed an argument about the BI, and without challenge (as this dissertation does), people may assume that the BI can be an error-free, neutral assessment of good and bad. An alternative screen, however, like surveillance studies can construct another narrative which questions the foundational assumptions of the BI such as its ability to predict the future, the idea that technology can help, and the idea that constant monitoring will make BIs "safer."

Burke and the Terministic Screen

One popular twentieth century rhetorician who helped shape this expanded view of rhetoric was Kenneth Burke. In the case of this dissertation, when I answered, "How does applying another terministic screen change the interpretation of the congressional

[9] As will be shown below, terminology often creates shared ideological assumptions through Burke's notion of *identification*.

communication," I used Burke's theory of the terministic screen to identify the alternative interpretation. By approaching the topic this way, I could explain one way in which BIs have been described as needing revisions but further the conversation with an alternative explanation.

Burke helped shift the focus of analysis from more basic understandings of Aristotelian appeals to looked at terminology in a more holistic sense which postulates that terminology specifically shapes and filters experiences. For Burke, humans attempt to use langue to make order in our world; we name things in order to control them (Burke, 1990). Due to the human desire to find common meaning amongst others, we look for unity through identification.[10] By agreeing on understood meanings of words and terminology, we are able to communicate with each other. We thus develop a shared terminology which creates a common ideology amongst collaborating groups. These ideologies are essentially shaped by the shared assumptions we make through language.

These shared ideologies though do not necessarily reflect a "true reality."[11] Just because one group agrees upon the shared meaning of terms doesn't mean another group believes the same or shares the same assumptions about these terms. As chapter one brought up, Burke (1945) points out that vocabularies are built on what is presumed to be "faithful *reflections* of reality" but these vocabularies are really just "*selections* of reality" and thus merely function as a "*deflection* of reality" (p. 59). In other words, whatever way arguments are constructed, this is just one choice of explanation and discourse. There are many other ways the "reality" of situations and experiences can be explained. One of Burke's oft-quoted expressions that exemplify this idea is: "Every way of seeing is also a way of not seeing" (Burke, 1984, p. 70). For each utterance and

[10] According to Blakesley (2012), Burke describes *identification* as "an alignment of interest or motives" (p.15), and for Burke, the main goal of rhetoric is identification. Burke (1969) illustrates this claim with his statement, "You persuade a man only insofar as you can talk his language by speech, gesture, tonality, order, image, attitude, idea, identifying your ways with his" (p. 55). We identify things to make sense of the world.

[11]As a caveat, a "true reality" is actually counter to the premise of rhetoric itself. As opposed to the philosophical view which sees knowledge as absolute truth with language as a tool, rhetoric looks at knowledge as contingent and created through argument and persuasion rather than discovered and absolute (Bizzel & Herzberg, 1990, p. 902).

explanation of an utterance there is a way in which the object of analysis was not described. Beach (2012) brings out that even half way through his book *A Rhetoric of Motives*, Burke stopped and wrote, "[L]et us try again…The best one can do is to try different approaches towards the same center, whenever the opportunity offers" (Burke, 1969, p. 137). Even Burke himself offered alternative accounts for what he was trying to explain. Overall, this shows that in both theory and practice, Burke followed the idea that people seek identification through shared ideologies, but in this attempt to find a shared ideology, one would also realize there were multiple, and competing ideologies.

In this sense then, language is seen as a construction depending on e.g., the society and speaker's proclivities. Depending on the ideology held, individuals will use words differently. Burke (1966) makes the distinction that this view of language has roots in dramatism (as opposed to the scientistic approach[12]). According to Burke, dramatism stresses the action behind language. Instead of seeing language and its words as external definitions or representations of truth, dramatism is more about social construction and involves the ideas of "thou *shalt*, or thou *shalt not*" (p. 44). Blakesley (2002) further clarifies Burke and explains that dramatism is more about action than just conveying information. Although people use language to communicate with each other, they use words "to define, persuade, appease, divide, identify, entertain, victimize, move [and] inspire" (p. 5). These words are rhetorical, persuasive, and incite others to action rather than absolute and representing an external Truth that just conveys information.

Burke, Terministic Screens, and BIs

Burke explains that settling on a particular way of thought is through the use of a terministic screen. Language then, and more specifically individual terms, are what composes arguments, and since language is a construction geared towards action though e.g., persuasion, the way one uses language is just one particular way of constructing an argument for action. For Burke (1966; 1990), terministic screens are lenses that we use to make sense of the world. How

[12] According to Burke (1966), the scientific approach concerns naming and/or defining a term and is more concerned with the idea something "*is* or *is not*" (p. 44). This approach treats language more as a tool to help facilitate communication rather than seeing language as a way to create action through actions such as persuasion.

we describe something is limited to our choice of terms and our shared assumptions about those terms in an ideological community.

Burke developed his theory in his work *Language as Symbolic Action: Essays on Life, Literature, and Method*. According to Burke (1966), our thoughts are shaped by the words we are thinking through. Burke likens the idea of these screens to filters put on photographs. If different filters were applied to photos of the same objects, even though the subject of those photos would remain the same, the way we saw them would be different depending on the filter that was placed on that photo. A photo with a red filter would look red, and a photo with a blue filter would appear blue. Similarly, for ideological or terministic screens, our words, terminologies, and ideologies we share shape and filter the way we perceive situations.

These screens are ultimately defined and limited by the terms we allow ourselves to use. According to Burke (1990), "[M]uch that we take as observations about 'reality' may be but the spinning out of possibilities implicit in our particular choice of terms" (p. 1035). Similarly, Herrick (2005) states, "Language, then, does not just describe truths, experiences, or ideas. Rather, it directs us to *look at* some things and *overlook* others" (p. 226). By naming things that now carry certain definitional expectations, we have defined one thing as not another thing and have provided a screen for understanding the world. What we call a dog we know is a dog because as a community, we share the same basic understanding of characteristics which make up a dog.

For this dissertation and the BI process, the terministic screen offers a valuable construct through which to analyze the congressional discourse about BI reform. The terministic screen encourages and provides a framework to analyze the same information in various ways. Specifically, for the idea of the terministic screen and BI reform, it is important to see the importance of a *term* and how one's term can be interpreted in different ways. To illustrate, as stated in chapter one, the term "whole person" is an important concept and emerges a goal for improving the BI procedure. As previously discussed, the whole person concept entails "a careful weighing of available, reliable information about the person, past and present, favorable and unfavorable" (*The Insider Threat*, 2013, p. 15). Throughout the documents, Congress uses the term the "whole person" and implies that this aim is essential to adjudications, and the more data

that is gathered about an applicant, the stronger BIs will be because there is more material to provide adjudication information.[13] The concept seems benevolent and outwardly looks as though the government is attempting to be fair and not discount an applicant simply because of one mistake.[14]

However, if one looks at the "whole person" concept through a lens of surveillance studies employing ideas such as social sorting, the idea that the "whole person" as a reliable gauge of character is called into question. Surveillance studies, and particularly Lyon (2009), describes social sorting (which will be discussed further in detail later in this chapter), as the use of databases and other classifications to profile groups to categorize them for particular methods of treatment. Looking at the terms "whole person" in conjunction with the terms "social sorting" helps put the idea of the "whole person" in another light. While Congress may think the whole person allows for a more thorough and fair investigation, this may not be the case. For instance, according to a House of Representatives report, the whole person concept looks at "what has happened in the person's life, what challenges they have faced, whether or not they have had issues with credit or alcohol" (*DC Navy Yard Shooting*, 2014, p. 58).

If one is thinking in terms of social sorting and the idea that people are sorted for profiles that allow for particular modes of treatment, the whole person concept becomes problematic. As shown above, the whole person concept is based on criteria such as credit history and use of alcohol. This assumes that those with credit and alcohol problems may be a threat to national security. In the case of finances however, the recession of 2008 shows that many individuals, formerly considered trustworthy, were faced with credit problems due to losing their job in the downturned economy.[15] The "whole person" is not just a problem (uncertainty about identity) and

[13] According to a House of Representatives report, the "whole person" "is critical in informing the adjudicator's determination of whether an individual should receive a security clearance" (H. Rep., 2014, p. 19).

[14] According to Henderson (2010b), the "whole person" concept attempts to provide mitigating information to possibly detrimental information identified in the adjudicative process. Also see the Center for Development of Security Excellence at http://www.cdse.edu/documents/cdse/121912-Webinar-Transcript_LC.pdf.

[15] There are times when some testifying in the documents under review do acknowledge the problems of using credit as a determining factor for the denial of clearances. For instance, David

solution (establishing character) when viewed as a way to facilitate sorting; the construction now becomes a way people are profiled based on criteria that may or may not make them a security threat. In order to believe the "whole person" problem and solution, one would have to believe the idea that alcohol and credit problems make an individual a security threat. Seeing the socially constructed nature of identity and risk is a conclusion that may not have been reached without applying a separate terministic screen which problematizes a particular term such as "whole person." Rhetoric and the terministic screen then are central to this dissertation to break down the congressional arguments. Without either, the "whole person" idea may go uninterrogated.

As seen through the "whole person" example, adding surveillance studies research to my analysis in this dissertation brings a new level of complexity. Since the theory of the terministic screen shows how one way of seeing is also a way of not seeing, surveillance studies is able to provide another disciplinary viewpoint to see the congressional documents in another way. Applying the terministic screen to the discussion helped reveal what is not explicitly said in the congressional documents and provided a more robust analysis of the reports in the study. As discussed in chapter one, because Snowden and Alexis betrayed the trust provided to them by their BI, the assumption was that somewhere along the way, their BI failed. The congressional documents selected for this dissertation address these failings and offer solutions within their particular screens and performative discourses. However, as will be discussed in chapter five, a surveillance studies lens shows how a failed BI may not be an explanation for Snowden or Alexis' actions, and BIs may not be flawed in the way Congress defines.

Borer, General Counsel for the American Federation of Government Employees stated, "Thanks to a 3-year pay freeze, sequestration in which over half of the Federal employees lost 30 percent of their take-home pay for 6 weeks, and a 16-day furlough with the shutdown, many were left unsure of how or when they would be able to pay their bills. Some untold number fell into debt or fell deeper into debt. (*Safeguarding Our Nation's Secrets*, 2013, p. 10). This statement does not have traction in the document in which it was discussed however, and during this hearing in relation to this comment, the discussion only focuses is how many Federal employees were actually stripped of their right to appeal terminations (due to matters like credit problems) after the court decisions of Kaplan V. Conyers. See https://scholar.google.com/scholar_case?case=15634329565788451072&hl=en&as_sdt=806 for more information.

Surveillance Studies

Lyon (2001) defines surveillance as "any collection and processing of personal data, whether identifiable or not, for the purposes of influencing or managing those whose data has been garnered" (p. 2). Restated, surveillance focuses on collecting information which in some way may have an effect on the behavior of the one under observation. The field of surveillance studies examines issues of surveillance, and one of its aims is to study how stakeholders (e.g., the government, corporations, and individuals) carry out surveillance practices. Much like the field of rhetoric which aims to examine how arguments are constructed, the field of surveillance studies also seeks to see how surveillance is constructed in both practice and discourse. Scholars do this by examining the actions of surveillance such as where surveillance is happening, why it proliferates, what is behind it, and who is affected (Lyon, 2007). Summarizing the field, Lyon, Haggerty, and Ball (2012) state:

> The contribution of surveillance studies is to foreground empirically, theoretically and ethically the nature, impact and effects of a fundamental social-ordering process. This process comprises the collection, usually (but not always) followed by analysis and application of information within a given domain of social, environmental, economic or political governance. Typically the process occurs through a series of interlinked, distributed and distantiated institutions, systems, bureaucracies and social connections. Consequently its effects are difficult to isolate and observe, as they are embedded within many normal aspects of daily life. (p. 1)

Surveillance thus studies attempts to isolate and observe these practices, stakeholders, and effects.

For the purpose of this dissertation, I used eight specific concepts from surveillance studies in order to see BIs as surveillance. I chose these concepts because they are prominent themes frequently discussed in the surveillance studies literature. These terms are constancy, surveillant assemblage, surveillers, social sorting, risk, prediction, identity, and technology. Each one of these filters helps see BIs (and the recommendations to fix them) as surveillance. A discussion of the field of surveillance studies, surveillance, and a brief explanation of each lens will help ground this study. Chapter four is more explanatory and compares these themes specifically to BIs to illustrate how BIs are surveillance.

As I began to touch on earlier, surveillance studies is an emergent interdisciplinary field, and one of the aims of the field is to examine surveillance practices which are either directly involved in watching particular groups or unconsciously embedded in daily life (Lyon, Haggerty, & Ball, 2012). These practices can range from friends watching each other on social media (Marwick, 2012), stores tracking purchases with loyalty cards (Gilliom & Monahan, 2013), OPM conducting BIs on candidates who willingly signed up for the investigations (USOPM Questionnaire for national security positions, n.d.), or metadata[16] being collected on Americans without their knowledge by the NSA (Lucas, 2014).

The field's treatment of surveillance may be different than what the non-expert may expect for a discussion of surveillance. For instance, a more mainstream definition of surveillance that comes up in a simple Google search is "the act of carefully watching someone or something especially in order to prevent or detect a crime" and "close watch kept over someone or something (as by a detective)" ("Surveillance," 2015). As opposed to Lyon's definition that began this section, these mainstream, Google search-understandings of surveillance often evoke the impression of criminals being monitored by the police or some other government or authoritative entity.

The differences between Google and Lyon's definitions are also illustrated through a search of images. Figure 1 provides a sample example of a typical result of a search for "surveillance." It is important to understand the differences between standard conceptions of surveillance and surveillance studies' use of the term because surveillance studies moves past the idea of surveillance as CCTV cameras watching anonymously from a street corner. Surveillance, among many associated concepts, has to do with theories, ethics, technology,

[16] The term *metadata* has roots in library and archival science and has been defined as "descriptive information used to index, arrange, file, and improve access to a library's or museum's resources" (Morville, 2005, p. 125). Regarding surveillance, as Snowden revealed, the government was keeping track of phone information about users such as phone numbers and lengths of calls ("Surveillance metadata," 2014). The collection of this information is highly contested though, and one reason, as per Richards & King (2014), is that now that storage is getting cheaper, corporations are storing information not just for what they can do now but for what they can possibly do in the future (p. 404). This topic is not explored at length in this dissertation due to divergent research questions, but it is an important and should be remembered as a point of analysis in surveillance studies.

history, society's tolerance, and social justice issues. It is not just institutions putting up cameras to watch the activities of those in physical spaces.

Figure 1. Surveillance image. Note: Data from Fleming (2010) under a creative commons license.

Similarly, results from searching "surveillance" images on Google visually reflect pictures of law enforcement and depict images featuring clandestine, secret shadowing where one must hide to evade scrutiny and surveillance technologies. ("Surveillance," n.d.). In the Google search results, the categories of pictures running across the top include the classifications of 1) Government; 2) Camera; 3) Signs; 4) You are Under; 5) NSA, and 6) Drones. In the government section, pictures begin with Uncle Sam iconography and range from the US government flag, security cameras watching the world, to an altered National Security Agency (NSA) emblem from the Electronic Frontier Foundation published on the *Business Insider* website depicting the emblem's American eagle clutching wires and listening with headphones (Braun, Flaherty, Gillum, & Apuzo, 2013). Pictures in the other categories include closed-circuit television (CCTV) cameras, signs warning that premises and properties are being protected by surveillance, warnings that one is under surveillance, the official emblem of NSA, and pictures of drones. Underneath these categories are images of control rooms with walls of monitors, pictures of CCTVs, a man hiding around the corner from a camera, employees watching CCTVs, an advertisement for security solutions, and

various technology associated with monitoring others such as cameras, CCTVs, and computer monitors.

These images represent popular sentiments, at least for Google algorithms, about surveillance. CCTVs act as constant reminders that one is being watched even without another human present. Drones can remotely watch populations from birds-eye vantage points. The images of hundreds of televisions showing CCTV camera feed illustrate the power of the watcher behind closed doors. Government emblems, altered or not, relate the idea that the government is conducting surveillance. As evidenced by the warning signs, too, we should be warned about surveillance, and although we may try to hide, there are always cameras there to see us and catch our behavior. Overwhelmingly, the images represent the watching of others from behind the scenes by people and governments in positions of power, and we should be alert and in a state of caution as the warning signs resulting in the search suggest.

Beyond Big Brother and the Panopticon

In addition to Google, these traditional ideas of surveillance also show up elsewhere, especially in pop culture. But again, these pop culture ideals do not represent current thinking on surveillance. One of the most popular and often cited examples in the depiction of surveillance is George Orwell's (1949/1950) *1984.* In *1984*, Orwell describes the character Big Brother, the supposed ruler of Oceana, as an authoritarian figure that monitors the citizens of the city everywhere they go and reminds the population through posters and other propaganda that they are under constant watch of a totalitarian state. The idea of Big Brother is so popular that it is even depicted in the first image of the "surveillance" Google search in the government section; this image, depicting Uncle Sam, reads, "Watching You" ("Surveillance, n.d.). This is very similar to *1984*'s catchphrase: "Big Brother is watching you" (Orwell, 1949/1950, p. 5).

For those studying surveillance though, a Big Brother-centered idea of surveillance is limiting. Surveillance is not just carried out by state actors conducting direct supervision of a specific, untrustworthy individual in a place of fear and caution. As Lyon (2001) comments, surveillance is *any* "collection and processing of personal data" (p. 2) for influencing and managing. Thus, for those that study surveillance, surveillance has moved from the specific

watching of untrustworthy individuals to being a broader collection of data on anyone. In part due to technology (amongst many other variables), surveillance has become easier and normalized, and nation-states are not the only entities large enough to have bureaucracies handling surveillance systems (Barnard-Wills, 2012). As stated above, surveillance can occur in any space such as social media or through supermarket loyalty cards.[17]

In addition to Big Brother, another popular concept often evoked when talking about surveillance is the Panopticon, and like Big Brother, those studying surveillance also discuss how this concept is also outdated and limiting. Michel Foucault theorized about the Panopticon, a prison design by Jeremy Bentham in the 18th century, and he tied its use to the idea of surveillance. Foucault often used the prison as an example of fear and control (Cohen, 1985; Foucault, 1977), and it became an allegory for institutional surveillance. The Panopticon in particular was envisioned as a circular building with a central, darkened guard tower in the middle. Because the prisoners in the outer rings couldn't see into the control tower, they never knew if there was a guard watching or not. This theoretically led the prisoners to control themselves and internalize the discipline (Staples, 2000). Similarly, Foucault saw this visibility imposed on all of society from many institutions. Institutions like schools, hospitals and employers watch their populations, and the people within those organizations hold themselves according to societal standards and become docile bodies based on their limited knowledge if someone was watching them or not.[18]

---

[17] Some may argue that essentially a loyalty card issued by a supermarket is still like Big Brother watching over the less-powerful; however, the idea of Big Brother I am referring to is specifically connotes the government, and a supermarket is not a government entity. Referring to Big Brother this way has precedence in Lyon (2007) who states Big Brother is a representative of the state which has "become pathologically absorbed with its own power and intimately involved in everyday control of its citizens' lives" (p. 32). Lyon offers the term *bureaucracy* to refer to a more general powerful entity not necessarily tied to the government. Further Gilliom and Monahan (2013) add that Big Brother no longer really makes sense because "surveillance comes not from a unitary state bent on only domination and control, but from a chaotic blend of government, media, work, friends, family, insurance companies, bankers, and automated data-processing systems. Much of the surveillance in our lives is non-threatening—hardly the sense we get from Orwells's classic dystopia" (p. 21).

[18] As a caveat, Foucault did discuss topics of resistance though, and fear someone is watching is not the only thing that keeps people obedient. According to Foucault (as cited in Aas, Gundhus, & Lomell, 2009) technologies of the self "permit individuals to effect by their own means or with the

Those studying surveillance see this idea as outdated too, though, and scholars see this for at least two reasons. First, ideas of the Panopticon are often tied to a centralized location. As discussed, the Panopticon architecture requires a centralized guard tower in one location overlooking a subjected population. Gilliom and Monahan (2013) challenge this idea however, and state about society, "We are watched not from a single site, but by many actors in many contexts with many motives" (p. 22). Second, the actors referred to are not limited to humans but now often include technology. Lyon (2007) states, "[D]espite what seem to have been Foucault's intentions, the idea of unilateral power vested in the inspector…has yielded a rather one-sided account of surveillance" which needs to be updated to account for electronic surveillance (p. 57). While Foucault may have been writing in the 1970's, he largely overlooked the machines that also watch our movements such as early computer technologies (Petersen, 2012). Surveillance sites are now digitized, and surveillance is should be seen as "mediated by electronic technologies" (p. 60).[19] As Walker Rettberg (2014) notes, technology becomes another member of the audience watching and taking note of what we do.

Overall then, both the idea of Big Brother and the Panopticon, two popular ways to theorize surveillance, are not the only way surveillance can be understood. Gilliom and Monahan (2013) sum up the argument and state, "The central idea is that *there is no central force: no Big Brother, no panopticon, but a shifting, moving observation, presentation, and regulation of the self by countless measures in countless locations"* (p. 22). Further, the dispersed nature of surveillance is often allowed through technology. In this way, contemporary power circulates in

help of others a certain number of operations on their own bodies and souls, thoughts, conduct, and way of being" to reach states like e.g. happiness, wisdom or perfection (p. 4). See Martin, L.H., Gutman, H. & Hutton, P.H. (Eds.) (1988) *Technologies of the self: a seminar with Michel Foucault*. Londong, Tavistock Publications for more information. In this sense then, individuals do have the ability to make their own decisions outside of fear.

[19] Gilliom and Monahan (2013) provide an example of this technological surveillance with the cell phone which can track "location, calls dialed and received, call contents, text messages, music, videos, photos, and all other transactions can be monitored or tracked by a shifting array of friends, family, service providers, private detectives, the police, or random strangers who find your phone" (p. 23).

ways that aren't rooted in one particular place (Nadesan, 2008). With technology, one does not have to be physically present to watch another.

As a caveat before continuing, just because these older and traditional models have given way to additional actors doesn't mean that older models have disappeared. As Lyon (2007) states, "[S]ome surveillance does still occur in enclosed spaces, above all in prisons, with which the diagram [of the Panopticon] was associated in the first place" (p. 61). Additionally, governments are still involved in tracking citizens, and according to Stalder and Lyon (2003), "[I]t is clear from the reactions to the 'terrorist' attacks of September 2001 that the older model can kick in at any time" (p. 90). Examples such as proposed mandatory government ID cards for either whole populations like in Canada or the UK or specific target groups such as refugees and immigrants show that the government is still invested in individually keeping track and monitoring its population (Lyon, 2009).

The BI example seemingly provides strong evidence of the more traditional idea of surveillance since the government is untimely responsible for conducting the investigations. For BIs, OPM is the agent of the clearances, and it's the government's objective to collect information on those undergoing the process. The government creates visible, structured models of surveillance like the example of Big Brother and the Panopticon. But just because BIs are seemingly conducted by a government entity, they are not that simple. As we see in chapter four, ideas of constancy, surveillant assemblage, surveillers, social sorting, risk, prediction, identity, and technology are all present in the BIs, and BIs aren't assembled through strictly government-entities.

Disciplinary and Control Societies

One way to differentiate among these shifting theories of surveillance is by breaking them down in two theses[20] often discussed in surveillance studies: the disciplinary society and the control society. The disciplinary society theory encompasses the ideas behind Big Brother and the Panopticon whereas the control society theory concerns the more fragmented and

[20] Lyon (2007) refers to the control society idea as a thesis (p. 61), so I use this terminology when referring to both ideas.

technological readings of the contemporary surveillance theories; understanding both of these theories helps differentiate between the two models of surveillance.

In his glossary of *Surveillance Studies: An Overview*, Lyon (2007) describes that in the disciplinary society, citizens control themselves in response to the possibility that someone is watching. Lyon (2007) goes on to say that this idea is discussed in Foucault's (1977) work *Discipline and Punish* which describes modern social control as being discipline-based. According to Foucault (1977), the disciplinary society was a change in perspective from more antiquated methods of control which focused on physical punishment and aimed to control the body through direct physical force in front of an audience. Torture as public spectacle and ceremonial punishment used to be a way to control a population, and the physical fear of being punished, in front of others, supposedly deterred future crimes. This spectacle was both a judicial and political move which aimed to brand the law breaker as deviant or take the life of the criminal, as proportional to the crime. Visible, physical punishment was a way to make sure the delinquent paid for his/her crime.

The disciplinary model moved away from this physical control however, and Foucault saw the disciplinary society as a type of control in which those under surveillance often internalized a fear of being watched and controlled their behavior due to this fear (much like the Panopticon illustrated).

On the other hand, the *control society* is a thesis that sees control not coming from specific locations such a guard tower or institution, but rather control is constant because of technological affordabilities that can track us everywhere. In a control society, one never leaves being monitored, and one is constantly being scrutinized. Wise (2002) illustrates this by saying:

> The barriers between home, work, school, prison, and the hospital begin to break down and run together…In a control society one could conceivably be at home, telecommuting into work, taking a telecourse, be on prison leave—attached to an ankle monitoring device—and be in the hospital—attached to monitoring devices that dial in to your doctor with your current vitals—all at the same time. (p. 32)

As opposed to Foucault and the disciplinary society's strong emphasis on institutions in brick-and-mortar locations with physical watching, the control society thesis is less about

embracing ideas of central stakeholders, unmediated by technology in fixed places.[21] Lyon (2007) states, "Whereas Foucault had theorized surveillance in the context of confined fixed spaces like the Panopticon, Deleuze proposed that such old sites of confinement were no longer the only or the primary sites of surveillance" (p. 60). [22] The model is more about maneuvering through a culture of control where surveillance is embedded in our daily actions through technology. Corporations, financial systems, social media sites, and loyalty cards: these all become surveillers who can keep track of individuals beyond their actual physical walls (if those even exist) through technological means.

Seeing outside of one's walls can lead to institutions knowing many things outside of their concern. For instance, a popular example of surveillance by a corporation through technological means is Target who developed an algorithm which identified the top items purchased by pregnant women (Duhigg, 2012). Once identified, Target would send coupons for baby care to the buyer. In 2012, this caused a problem when a teenager's father was upset that his daughter was receiving the coupon book. The father believed his teenage daughter was being inappropriately targeted as a mother-to-be; however, the father did not realize his daughter was in fact pregnant. This example illustrates the corporation's ability to know details of its customers outside of its physical location due to technology.[23]

Due to this institutional breakdown of control, a nation's ability to surveil its citizens can be seen as almost endless. Control and monitoring are no longer isolated to certain institutions, and it seems that people can be monitored at all times from a variety of places, be it through social media, loyalty cards, official OPM BIs or the recording of metadata. This control has come to a point where Wise (2002) concludes, "[O]ne might wax nostalgic for a disciplinary society

[21] Further, according to Wise (2002), in a disciplinary society "apparatuses start over at each site," in a control society, "control is continuous" (Wise, 2002, p. 32) because technology can transcend institutional boundaries.

[22] Gilles Deleuze (1992) provides a deeper discussion of the control society.

[23] While this example shows how surveillance may be embedded passively through things like shopping habits, technology may also allow for more aggressive surveillance such as when state authorities set up "technological and policy architectures that facilitate state control over the Internet" (Kalathil & Boas, 2003, p. 137).

because in that society at least there were limits to control; one could leave school and go to work" (p. 32).

Surveillance studies tends to embrace the second thesis of the control society. I also adopted principles of the control society for my dissertation, and again, I looked at eight specific areas emerging from surveillance studies which I chose to explore further as a lens or terministic screen for the congressional documents. As stated, these terms are constancy, surveillant assemblage, surveillers, social sorting, risk, prediction, identity, and technology. I will now provide a brief discussion of each lens in order to understand their meaning in my dissertation.

Constancy

The first concept I analyzed was constancy. Constancy is a recurring theme in the control society which, as stated, is a prominent thesis employed in the field of surveillance studies. As Lyon (2007) stated, in a control society, "electronic technologies increasingly permit constant and mobile surveillance across spheres of everyday life," and computers can now track people all the time (p. 199). Because the control society thesis concerns constant monitoring, in this control society lens, there is a constancy to surveillance that one can never get away from. Surveillant practices take in information about a population continuously, and despite traveling from institution to institution, there is the belief that we can always be surveilled.

For the purpose of this dissertation, the filter of constancy was used to identify places in the BI reform documents where control is illustrated by practices of continuous monitoring. As an example from my study, OPM's FIS Associate Director Merton Miller provides an illustration of this in a 2014 House of Representatives report when he states, "We think that's the future of background investigations, where you don't ever close a case…[I]t's a living document. It never closes. We're going to constantly update that information with information that's relevant to your character and conduct" (H. Rep, 2014, p. 34). Further, Representative Gerald Connolly adds this continuous monitoring is common sense, and would include a more frequent, random automated review of public records and databases because "today we have the technology to make more continuous monitoring work" (*DC Navy Yard Shooting,* 2014, p. 150). The statements show that constant monitoring is a goal for BI reform, and ways to achieve this are through technological

observation. This example shows that while Congress is offering their narrative of reform, a different interpretation of the same documents surfaces when the documents are viewed through a concept such as constancy. Whereas Congress sees constant monitoring as a solution, a surveillance studies understanding of continuous monitoring reminds us that constancy is just another characteristic of a society of control.

Surveillant Assemblage

The idea of constancy leads in to the idea of surveillant assemblage. This concept, popularized by Haggerty and Ericson (2000) in their seminal piece "The Surveillant Assemblage," is concerned with understanding how information is gathered for surveillance purposes. If, as described above, we are constantly being monitored by a vast number of players as opposed to one, centralized institution, the information gathered from these locations is vast, may be seemingly unalike, and may not seem to make connections with each other. These pieces of information are what make up modern surveillance practices, though, and after being turned into digitized information, these parts are reassembled and gain meaning by whomever has the information and for whatever reason the information is being reassembled. This meaning is further dependent on the databases the information lies within and the agenda of those controlling the database.

An illustration of surveillant assemblage will hopefully make this clear and tie all these ideas together. While a grocery store may be gathering purchase information about an individual through loyalty cards in one specific store or for one chain of stores, an internet service provider may be gathering information about the same person's browsing history. Both of these sources of information could be used for influence or management (surveillance) purposes, but they are taken from different places, and may seemingly be unrelated. If, however, information from both of the sources gets inputted into a more singular database, this information compilation (or assemblage) can take on new meaning and be used for additional surveillance purposes. A marketing firm able to get both sources of data may be pleased to use this information to determine what products to market, but a police department obtaining the data may be more interested in seeing if a suspect purchased duct tape after searching how to kidnap someone.

The database could thus be seen as an assemblage of surveillance information by gathering seemingly incongruent sources of information, but the meaning assigned to the information differs depending on who controls the data. Surveillance assemblage then entails getting information from many places, and unlike Big Brother or the Panopticon, it is not necessarily from a government entity in a physically fixed location.

To explain more in depth, Gilles Deleuze and Felix Guattari (1987) discussed the larger term of *assemblage*, and it is based on the idea that information is fluid, changeable, and moveable. According to Wise (2005), assemblage is neither a random collection nor a predetermined compilation of things; it is a process of organization which creates a territory that has a claim or expression. Thus, the process (or assemblage) of putting together a compilation of different things creates a territory which exists only in the compilation of these parts. These assemblages are not fixed and solid groupings either; they are different combinations of data that can be reconstructed in different ways to form different assemblages. The ways assemblages are reconstituted determines their meanings. The information gathered on an individual would claim a territory about that individual, and depending on who controlled the database where the information was reconstituted, there would be a different meaning assigned to the information.

Building off Deleuze and Guattari (1987), Haggerty and Ericson (2000) coined the term "surveillant assemblage" which refers to seemingly unrelated data flowing from multiple sources that are "reassembled and scrutinized in the hope of developing strategies of governance, commerce and control" (613). Like assemblage, *surveillant assemblage* is concerned with compiling different sources of information (in this case surveillance information) into territories which can form multiple assemblages, and the meaning for surveillance depends on how the assemblages are reconstituted.

In addition, this information is often in the digital form. Surveillant assemblage doesn't just gather information from various sources, but it also involves the digitization of this information so that it can be reassembled in databases. Haggerty and Ericson (2000) state, "[S]urveillant assemblage relies on machines to make and record discrete observations" (p. 612) and is concerned with "transforming the body into pure information, such that it can be rendered more

mobile and comparable" (p. 613). It is not just the various sources of information then that make up a surveillant assemblage; it is also the fact that the information is digitized and flows, independent of where an individual actually physically is, into various databases for the purpose of surveillance.

On the surface for BIs in particular, they are formed through assemblages because the surveillance data that composes them are from disparate sources of information such as candidate interviews, proof of date and place of birth, corroboration of education and employment, interviews with coworkers and neighbors, national agency checks, financial review, law enforcement, and many other different factors (USGAO, 1999 & 2000). For an example specifically in the documents under review for this dissertation, the House of Representatives issued a statement which said federal agencies need "real-time access to critical information relevant to background check investigations, including arrest records, court records, financial credit history, currency transactions, foreign travel, social media, and terrorist and criminal watch lists (*DC Navy Yard Shooting,* 2014, p. 140). As shown, each source of information about the individual under consideration for a clearance is flowing from a different source and forming a territory due to the institutional requirements of OPM. The subject of investigation then is made up of flows of information which come from various, seemingly unrelated sources through digital means.

Surveillers

The third concept I analyzed was surveillers, or those doing the surveillance. As discussed in the previous section, the idea of surveillant assemblages in surveillance studies is different than popular surveillance metaphors like Big Brother and the Panopticon which rely on centralized and singular entities collecting information (Haggerty & Ericson, 2000). For Big Brother, there is a totalitarian state looking at everyone's movement, and for the Panopticon, there is a single site of brick and mortar observation (Gilliom & Monahan, 2013; Haggerty & Ericson, 2000). Surveillant assemblages on the other hand expand surveillance from the idea of one watcher to a larger network and flow of information coming from multiple places, and the government is no longer the primary stakeholder involved in surveillance practices.

This expansion fundamentally changes the players and definitions of surveillance. As discussed, rudimentary Google searches of definitions and images often depict surveillance as the government or law enforcement as the surveilling stakeholder. Lyon (2003a) points out that the word "surveillance" used to mean "specific scrutiny of subjects such as police wiretapping or foreign intelligence" (p. 1), and Barnard-Wills (2012) comments that classical and popular understandings of surveillance often position the state as the main entity conducting surveillance. In this shift though to more of an assemblage-based thesis, the government no longer remains the only entity conducting surveillance, and other entities like corporations or even regular citizens can surveil each other. This modification thus breaks down the hierarchical, central power and shows how multiple, non-governmental players supply various flows of information. There is no longer just a view of surveillance where surveillance is carried out by a totalitarian state (like Orwell's (*1984*) or watching in a confined, institutionalized, fixed location (like in Foucault and Bentham's Panopticon model). Instead, information comes from multiple sources in various locations. This information is reassembled in databases (Gates, 2011) in places like law enforcement facilities, financial centers, Amazon or Netflix facilities, or at Google. Terms like coveillance, sousveillance, and dataveillance[24] highlight the non-state stakeholder as surveiller where those engaged in surveillance may be peers (coveillance), those not in positions of power (sousveillance), or from machines (dataveillance).

As a caveat though, just because there are more stakeholders involved in surveillance along with the government, the situation doesn't have to be an either-or scenario. Newer ideas of surveillance don't mean that either conception is mutually exclusive of each other. Stalder and Lyon (2003) comment that the older state-centered model can utilize other sources of surveillance data for their own ends (p. 90), and for instance, the government can use non-state

[24] Sousveillance is a term coined by Mann, Nolan, & Wellman in 2003 is the idea that citizens watch those in power (as opposed to the powerful watching the powerless), and coveillance is a form of sousveillance but in this instance, citizens watch each other (Mann, Nolan, & Wellman, 2003). Videos shot by citizens of police brutality would be sousveillance, and coveillance can be a peer taking a picture of another peer. Dataveillance was developed by Roger Clarke (Clarke, 2013), and it involves watching that is not by sight but rather automated, personal data systems which are compiled to create "seen" profiles (Lyon, 2007).

entities in order to gain surveillance data. For example, as discussed in the previous section, Congress wanted federal agencies using data from "financial credit history, currency transactions, foreign travel, social media, and terrorist and criminal watch lists" (*DC Navy Yard Shooting,* 2014, p. 140) which may or may not be from non-government sources. A credit bureau like Experian and a social media site like Facebook are not run by the federal government, but they could be sources of information.

For this dissertation in particular, this point can be seen in the breakdown of the BI process. BIs are one strong example of the change and melding of surveillant actors. BIs are conducted for OPM, but as discussed earlier they use data from everyday sources like credit reports and social media in order to conduct complete this surveillance. Also, in addition to incorporating sources of data from different and non-government databases, those involved in conducting the investigations are also not always federal employees. As of 2014, 70% of OPM's investigations were conducted by contractors (H.Rep, 2014; *DC Navy Yard Shooting,* 2014). So despite the tradition appearance of government-sponsored surveillance, even the BI is a compilation of various stakeholders who are not all part of the government.

Social Sorting

Social sorting is another concern of surveillance studies and a lens I applied to the selected texts. After information is gathered by multiple stakeholders from multiple locations, something has to be done with this information in order for it to be usable. As Lyon (2001) stated, surveillance is "for the purposes of influencing or managing those whose data has been garnered" (p. 2). The use of this information for influencing or managing means that some type of interpretation needs to be made about this information. This meaning-making can be described as social sorting. Sorting involves putting things in categories in order to manage and control them. According to Lyon (2009), social sorting is one of the main threads of surveillance studies, and involves "the use of searchable databases and associated techniques such as data mining, characterized by the classifying and profiling of groups in order to provide different levels of treatment, conditions or service to groups that have thus been distinguished from one another" (p. 41).

Essentially then, after information is assembled, meaning is ascribed to categorize and use this information. In a more benign example of sorting, say a Netflix watcher watches only comedy movies. Then their computerized Netflix browsing history may be sorted into a category of a user that likes comedies, and Netflix algorithms may subsequently suggest to the user more comedies to watch. In a more problematic example, an individual that has had credit problems in the past may be denied a loan for the future even though their credit problems may have only stemmed from a medical issue that has since been rectified and does not reflect a carelessness for debt repayment. Sorting is such a big part of surveillance that Bauman and Lyon (2013) conclude, "*Social sorting* is primarily what today's surveillance achieves" (p. 13). It most importantly leads to some type of determination of action, or as Lyon says, treatment, conditions or service. Based on how the information is assembled and sorted, the individual will be judged and classified.

The fact that the material is digitized and exists in a database is also important to the idea of social sorting (Lyon, 2003b). Gordon (2011) adds that the database itself is inherent to the definition of social sorting and social sorting "refers to a variety of surveillance practices that create various databases and have access to others--public services, police, intelligence, business, consumers - in order to categorize people for different treatment" (p. 167). Oscar Gandy was one of the first people to talk about the use of technology to sort individuals in his book The *Panoptic Sort*. Gandy (1993) explained that surveillance and sorting was under the control of an "all-seeing eye of the difference machine" designed to sort people based on routine measurements in order to provide or deny opportunities (15). Sorting also involved categorizing the digitized, databased information based on institutional preferences through pre-determined computer algorithms created by the entity using this information. Thus, computer codes become very important pieces of the process of surveillance and sorting, and as Lyon (2003b) succinctly says, "[S]urveillances systems are what are in the codes" (p. 23). Working backwards then, codes become the way people are filtered for advantages and disadvantages. Databases are the ways people are organized, and surveillant assemblages provide the content for the surveillant decisions resulting in gains or losses.

These advantages and disadvantages are also viewed as overwhelming problematic. In surveillance, sorting people into groups can lead to problems. One way it is problematic is if information is inputted incorrectly in a database in the first place. For instance, there are cases where individuals are erroneously sorted onto no-fly lists (Lyon, 2007; Gilliom & Monahan, 2013). Additionally, many times individuals may be placed into categories of risk despite that they have not yet committing any wrongdoing. Staples (2000) adds that not only "deviants" are under the gaze of control; surveillance data produces "'types' or whole classes of individuals who are deemed 'at risk' for behavior" (p. 6). For example, a shopper with a credit history at a bar, massage parlor, casino, pawnshop, and bail bondsman may be categorized as a financial risk even though they have never had any financial troubles (Gilliom & Monahan, 2013). They may be categorized as a potential threat or considered under "categorical suspicion" because they are grouped into a suspicious class (Lyon, 2007). Even more problematic is that often the data or risk factors used in algorithms to sort people are features people have little control over such as information based on "age, race, ethnicity, gender, and chronic disabilities" (Ericson & Haggerty, 1997, p. 120). This can lead to profiling based on inaccurate assumptions and prejudices.

For BIs, one example of social sorting involves the overall purpose of the security clearance: either granting or denying a clearance. Depending on the assemblage of surveillance information, a person will be sorted to either get access or be denied a clearance privileges based on the requirements in the codes of the institution. As an example from the documents under review, according to Greg Marshall, Chief Security Officer, U.S. Department of Homeland Security in a House of Representatives report, "If derogatory information reached us, and it was deemed to be good information, we would deactivate their card, both their card and also the access system. We would bring them in and read them out, if they had a security clearance, we would read them out. So they would not only not have access to Classified information any longer, they would also not have access to facilities" (*Facility Protection,* 2013, p. 33). Thus, the individual would be sorted into a specific category with predetermined access allowances. Based on information obtained about an individual, the individual would receive specific levels of treatment corresponding to whether they were denied/allowed a clearance.

Risk

Underscoring many goals of surveillance is the idea of risk. In fact, Lyon (2001) describes that "[s]urveillance is the means whereby knowledge is produced for administering populations in relations to risk" (p. 6). Barnard-Wills (2012) further adds that surveillance provides the data for risk assessments (p. 178). Sorting then is based on the perception of risk. Risk becomes the justification for actions taken based on surveillance data.

Depending on how an institution with surveillance data sorts the assemblages of information, they will react and sort the individual into a category of (dis)advantage based on the data. For instance, as in the example above, a bank loan applicant with a poor credit history may be sorted into a category of a risk, and the individual may be denied a loan. The potential for something bad to happen makes the individual too risky for an advantage. Similarly, the idea that there were red flags for Alexis and Snowden (Enhanced, 2013; *The Insider*, 2013) suggests that these individuals were too much of a risk for the surveillance system and should have been denied a clearance.

Risk is a complicated idea and a concept towards which a whole compendium of literature is devoted. Before delving onto surveillance studies' discussions of risk, it is helpful to see a larger picture of competing concepts of risk. Lupton (1999) characterizes attitudes towards risk in three ways: realist, strong constructionists, and weak constructionist (p. 35). Realists see risk as being independent of cultural and social issues. According to Ekberg (2007), "Realists argue that risks are real. Risks can be identified, measured, classified and predicted by following rigorous, reliable and reproducible methods and calibrated techniques of the quantitative sciences" (p. 348). Strong constructionists on the other hand take an opposite stance and theorize that there are really no risks in themselves, and risk is just a label society places on certain things, all dependent on social and political issues (Lupton, 1999). Ewald (1991) synthesized this stance by commenting, "Nothing is a risk in itself; there is no risk in reality. But on the other hand, anything *can* be a risk; it all depends on how one analyses the danger, considers the event" (p. 199). In this since, risks only exist in definitions. Lupton's (1999) third categorization is the weak constructionist who sees risks as existent objectively, but these risks

can never be seen isolated and must be viewed through cultural and social practices. Ulrich Beck (1992), a leading theorist on risk subscribed to this idea (Lupton, 1999, p.60) and alluded to this when he stated that risks are *"open to social definition and construction*" (Beck, 1992, p. 23, emphasis is original). Risks then may exist in a physical sense, but they are *open* to interpretation due to sociological factors.

Surveillance studies often takes the weak constructivist view as evidenced by the discussion of social sorting. While risks are thought to exist, the risks are only identified when filtered through the lenses of the institutions which are interpreting the assembled surveillance data. Risks may be present, but they are only articulated as risks when a particular institution deems them as a risk.[25]

An important work in surveillance studies in the theory of risk comes from Ericson and Haggerty's (1997) book *Policing the Risk Society.* In this book, the two define risk as "external danger, such as a natural disaster, technological catastrophe, or threatening behavior by human beings" (Ericson & Haggerty, 1997, p. 3). In this sense then, risks are thus things to avoid. The authors further show that in order to avoid taking on more risks, risks are identified and communicated through risk communication systems which consist of "rules, formats, and technologies" (p. 4) which institutions use to define risk. To understand an organization, one must understand what institutions consider risks. For instance, if a police department deems broken windows a risk to the community's safety, then the department's policies, rules and technologies will be devoted and focused towards eliminating the broken windows. On the other hand, another department may feel higher level crimes should be pursued and attention is not placed on broken windows since the department does not see this element as a risk. Thus, the risk communication system helps define and focus attention to certain risks.

In the case of BIs, the congressional reform documents often use the term risk, and the texts also outline the risk management systems that the government employs to keep risk

[25] As an aside, this constructivist idea also harkens back to Burke's view of rhetoric as a terministic screen because institutions are turning some risks into *risks* while turning their attention away from other things that could be declared *risks.*

minimized. There are many executive orders and legislative controls which outline the processes of BIs and are designed to standardize the BI process. Risk gets communicated through these policies and lawmaking procedures. Thus, this discussion of risk and understanding the theoretical differentiations of what constitutes risks helps show that in the case of BIs, risks can be seen as just social constructions rather than risks that exist on their own and without interpretation.

For this dissertation, I examined what the congressional documents consider to be a risk and how those risks are communicated to others; in the documents under review, there was much discussion about what topics are considered risks and needed further clarification from an applicant. For instance, according to Senator Tom Coburn in a Senate report, the form used by OPM to initially gather information used to begin the BI has "three pages of instructions, seven pages where you live, five pages of names, 17 pages of employment, four pages of military, 29 pages on relationship, 21 pages on foreign activity, two pages on emotional health, seven pages on police records, 11 pages on drug and alcohol, eight pages on financial records, five pages on associations, and three signature pages" (*The Navy Yard Tragedy,* 2013, p. 21). This statement not only shows that OPM has a methodical approach to surveillance organized around many checkpoints, but also, each of these checkpoints helps define what OPM considers a risk. If these points were not potentially important for BIs, then they would not be included on the clearance application. The form thus defines risk and helps OPM carry out procedures set to minimize risks.

Prediction

Risks attempt to predict the future, so prediction can be seen as a byproduct of surveillance. In order to get data to sort through, data must initially be gathered, which as described, is through surveillance. Data from multiple institutions gets combined into databases and then sorted and assessed based on institutional preferences. If there is a probability that an individual may deviate from desired behavior (i.e., divulge classified information rather than keep it secret), then the individual is considered a risk and may not get the advantage of whatever they are trying to obtain. Sorting the individual into a category where they are denied an advantage thus tries to prevent future adverse behavior.

Surveillance studies' discussion of policing is one major illustration of the nature of prediction in risk. According to Lyon (2007), policing today tries to prevent crime before it occurs and "depends on information, on gauging probabilities, on a risk calculus and on algorithmic methods" (p. 40). Prediction is so engrained in policing that by the late 20th century, Gary T. Marx (2004) concluded that we are entering a new form of surveillance which is moving us towards a "maximum security society"[26] where rather than, according to Lyon (2007), being policed after they have committed a crime, people are "contingently categorized" as possible risks (p. 107). According to Lyon (2007), this situation means that they are placed in categories of suspicion[27] and only cleared when a system says they are safe.

This categorization can be detrimental to those identified as posing a risk to society. The idea of profiling especially illustrates this. In some cases, law enforcement has been known to place extra scrutiny on segments of the population just because they are categorized at increased levels of risk, and profiling illustrates that some people may be sorted into types of people that technology has decided may do something in the future, but yet, they are currently not guilty of anything. According to Ericson and Haggerty (1997), there is a "history of governments producing knowledge about race and ethnicity to discover statistical laws that allow policing of racial and ethnic groups" (p. 282). Also, as the stated earlier, risk information is often based on "age, race, ethnicity, gender, and chronic disabilities" (p. 120). These predictions are thus discriminatory and could be based on factors that aren't even relevant to making decisions. Ericson & Haggerty continue, "People are excluded from risk pools by statistical probabilities that

[26] Marx (2004) describes this type of society as being: "1) a *dossier* society in which computerized records play a major role 2) an *actuarial* society in which decisions are increasingly made on the basis of predictions about future behavior as a result of membership in, and comparisons to, aggregate categories 3) a *suspicious* society in which everyone is suspected 4) an *engineered* society in which choices are increasingly limited and determined by the physical and social environment 5) a *transparent* society, in which the boundaries of time, distance, darkness, and physical barriers that traditionally protected information are weakened and 6) a *self-monitored* society, in which auto-surveillance plays a prominent role."

[27] According to Lyon (2007), categorical suspicion describes a designation where certain groups are identified as potential offenders, and "simply inhabiting a categorical niche is enough to attract suspicion" (p. 106). This is similar to Staples (2000) who identified that surveillance data produces 'types' or "whole classes of individuals who are deemed 'at risk' for behavior" which moves punishment from the individual deviant to the overall "type" (p. 6).

often rely on poor or false indicators of offending behavior. Unable to take into account context and circumstances, these technologies either misrepresent them or simply fill in the blind spots with local bureaucratic custom" (p. 122).

To illustrate the idea of statistic probability, NPR aired two stories about the use of computer statistics to determine where crimes can occur. In one story, police in Peoria, AZ were using the program HunchLab's algorithmic technology to see where crime patterns exist and use predictive policing "to take a look at where crime may occur as opposed to the crime that has already occurred" (Bernier, 2016).[28] Additionally, NPR also ran a story about Texas' use of algorithmic technology and predictive analytics to predict child abuse, and in this case, "the technology identified specific locations in advance, actual blocks in a neighborhood, where cases of abuse would occur" (Silverman, 2016). Both of these examples show that certain areas and the people that live within the predicted zones may be targets of surveillance, not by what they have done, but rather because technology has identified their area as a greater risk. Risks then, when attempting to predict the future, may really only be discriminatory in practice rather than quelling future harm.

For this dissertation, prediction is an important factor to consider because prediction supposedly failed when it came to Snowden and Alexis. When making recommendations to fix the clearance process, according to Senator Susan Collins, "The OPM Background Investigation process must be capable of flagging high-risk individuals holding clearances and alert case officers of situations requiring review before any adverse consequence takes place" (Enhanced Security Clearance Act of 2013, 2013). Thus, change was needed after Snowden and Alexis because supposedly the system was not strong enough. Snowden and Alexis weren't identified as high-risk. This can be seen further when Collins continues:

> If random audits had been in place after Aaron Alexis's secret clearance was granted in 2007, red flags would have been generated with his arrest in 2009 and the two liens on his property, which could indicate potential excessive financial hardship. Further, it may have identified a potential alias with a vast social media trail indicating other concerning

[28] The claim is that HunchLab technology supposedly is "essentially eliminating bias" (Bernier, 2016). It would be interesting to explore this claim further, but this would not be in the scope of my current dissertation.

> traits. The alerts generated would have prompted OPM to notify DOD, which would have provoked a reevaluation before Alexis's 2017 re-clearance. This re-evaluation could have discovered that he openly discussed "hearing voices," a clear sign of his mental illness. A random audit would have alerted OPM of these new issues and potentially averted tragedy. (Enhanced Security Clearance Act of 2013, 2013)

Despite these claims though, it is impossible to know whether a different process may have stopped Alexis from his behavior. These passages are representative of many other passages throughout the documents under review though, and the idea that behavior could have been predicted permeates the recommendations for changing the BI process.

Identity

Identity was the seventh lens I applied to the dissertation texts. To recap, in a control society, individuals are constantly monitored, and their information is gathered from a variety of sources. This information is assembled in various locations, by multiple players, in order for sorting based on risk profiles, to predict the future. These profiles ultimately become their institutionally constructed identities and establish how an individual is defined based off the data gathered about them. Surveillance practices are thus attempting to make some sort of identification about those under the surveillance gaze. At the core of surveillance then is an attempt to establish identity (Barnarnd-Wills, 2009; Bennett, Raab, & Regan, 2003; Stalder & Lyon, 2003).

When looking at examples of identity within surveillance practices, oftentimes, the individual under surveillance is not in control of constructing their own identities. For instance, I may have watch only comedies on Netflix due to coincidence, but Netflix may consider me a user that likes comedies even though I don't identify as a comedy lover. The institution says I like comedies even though I don't really enjoy watching comedic movies. Maybe the only comedies I watched were in social settings where someone else picked the movie through my user profile. Netflix doesn't see the context of my choices, and they just assume that by the data I am a comedy watcher. My identity was thus constructed by the institution.

Another example of an institutionally constructed identity (in this case government) is idea of a national ID card. Thinking about driver licenses (DLs) in the US, this ID relays one's photo, assigned ID number, name, date of birth, address, and also links to a database which also

provides additional information such as driving history, warrants, and other possibly pertinent information. The license becomes an extension of oneself; it represents a static, namable identity. If law enforcement were to run my DL through their systems, I would become to them who their database said that I was. There is a belief in a static entity of an individual, and the ID card can relay this information (Lyon, 2009).

As a field of inquiry, surveillance studies tries to bring attention to the more constructed, external nature of identities and often draws attention to the idea that identities really only emerge in certain contexts (Barnard-Wills, 2009, 2012, & 2014; Lyon, 2009). As social sorting, risk, and prediction illustrate, due to algorithms and institutional filters, identities are often related to the preferences of those using the data and not necessarily a preexisting identity.

Lyon's (2009) differentiation of *identity* versus *identification* helps to see the difference between an identity one picks for themselves versus one that is imposed upon an individual. Lyon argues that these two terms of *identity* and *identification* are not the same. For instance, for Jane Doe, *identification* refers to what happens when her ID is taken by a law enforcement official, bartender, prospective employer, or anyone else looking to verify that she is Jane Doe. The DL shows how her featured photo matches to her physical presence and affirms that she is who she says she is. *Identity*, however, is less formal and involves more personal descriptions of a person's background and history. Jane's identity is not solely made up of a birthdate and potential parking tickets that she may hold; it is more concerned with who Jane feels as a person. Jane identifies as being an American, Arizonan, animal lover, atheist, altruist; all things that are more personal affiliations about one's sense of self rather than information used for identification purposes often ascribed by outsiders (e,g., one doesn't get to select a DL number or give themselves parking tickets – these are imposed by outside forces). Identity is a more constructed sense of self Jane gets to put on herself rather than a description of her character levied upon her. Identification is more of a process of verification where a DL is a tool; it is a more formal attempt to keep track of individuals for the purpose of management.

Surveillance studies also emphasizes that the chance to assert our identities rather than be identified is greatly reduced in the control society due to the way identification is

impersonalized through technology. As stated above, the control society utilizes technology so that an individual is constantly under surveillance of some form, often technologically. Surveillance assembles data from multiple sources, and information goes into a database where the information is arranged and socially sorted based on a particular institution's often algorithmic preferences in order to hopefully predict and eliminate potential risk. Once an individual is sorted into a particular category, these assemblages then, formerly fluid and changing, coalesce into a more permanent, be it virtual, form of the subject.

This permanent, virtual self can now be considered what (Haggerty & Ericson, 2000) call one's *data double*. The data double is a new version of the self, a digital version which now exists in codes and technology rather than one's identity of self. It becomes one's identification and not identity. One no longer gets to really relay to these decision-making institutions about their identities and who they feel they are; they are limited to what their database codes about them.

In order to create a data double, Haggerty and Ericson (2000) comment regarding the observed body, "First it is broken down by being abstracted from its territorial setting. It is then reassembled in different settings through a series of data flows. The result is a decorporealized body, a 'data double' of pure virtuality" (p. 611). The body thus gets taken apart and analyzed in different places by different methods; it is removed from its original setting, and it is then brought together again and a newly-formed way. It is no longer the body of the individual, but it contains information from that original body. These data doubles then become "markers for access to resources, services and power in ways which are often unknown to its referent" (p. 613). They are comprised of information which is ranked according to how useful they are in allowing institutions to discriminate (as in placing things in certain categories based off of institutionally-defined criteria) (Lyon, 2007). The body then gets separated from the data double, and *identification* becomes predominant. Jane Doe trying to get a loan is now made of her credit score stored in databases controlled and ranked by a bank rather than providing her identity and feelings about her credit worthiness. For a bank loan, her character is less about who she thinks she is and more about who her code and algorithms say she is.

Applying these theories of identity as a lens through which to the congressional documents shows how Congress' recommendations for reform are also about constructing identities. BIs and their suggested restructurings are involved in positioning applicants in certain ways for certain gains or losses. To illustrate this using the congressional documents, according to Gregory Marshall, Chief Security Officer at the US Department of Homeland Security, "Based upon all available information, a personnel security specialist makes an adjudicative decision concerning a person's suitability or fitness for employment" (*The Insider Threat to Homeland Security*, 2013, pp. 13-14). This statement shows how identity is imposed from the outside; one is surveilled by a background investigator, and the intelligence from that investigator goes to an adjudicator.[29] The adjudicator, without ever meeting the clearance applicant, then establishes the trustworthiness of that applicant.[30]

Technology

The final lens I applied for this dissertation was technology. As can be seen in a Google image search of "surveillance" ("Surveillance, n.d.) when the issue of surveillance is brought up in more mainstream conversations, technology is usually associated with the descriptions. Almost all of the images in a Google search of "surveillance" involved some image of technology. There are CCTV cameras, drones, control rooms full of monitors; all of these machines are designed to keep watch on populations and gather information about what is going on.

Technology is thus something of importance to consider when studying aspects of surveillance. Technology helps explain how processes are able to be carried out and how tech has changed the practice and thesis of surveillance in general. Technology ties all of the major themes discussed together: technology helps to continually monitor for the purpose of control, assists in storing data in databases for surveillant assemblages, assists as a surveiller in the

[29] See Figure 2 for additional information on the Federal BI process.

[30] As an additional example, also recall the previous discussion on the "whole person." Adjudications are based on the idea that a whole picture of an individual has been established through investigation. The adjudicator supposedly then has all the data about an individual in order to make an informed decision about a clearance.

gathering of information, helps socially sort populations with algorithms, helps to control risk and predict the future, and helps assign identities through sorting (Lyon, 2007).

Literature on surveillance complicates the overall connection between technology and surveillance though. Although as stated the field utilizes the control society thesis which shows that surveillance operates through technology for constant monitoring, the field also emphasizes that there is a human element to the collection and review of surveillance data regardless of how neutral technology may seem to be (Humphreys, 2011; Kim, 2004; Smith, 2008 & 2012). Technology always has some type of human footprint and is not an impartial or an unbiased surveiller that extracts information without an addition of some type of interpretation. Technology does not spontaneously come into existence, and data in these systems are subject to their own terministic screens. Both of these elements depend on how computers are set up and programmed.

This is especially seen in the databases and algorithms that store and sort surveillance information. Gates (2011) provides the example of facial recognition technology and its dependency on human intervention. TV shows may portray detectives entering in the face of a suspect into a database, the database does searching, the photo comes up as a match to a particular identification, and a case is solved. However, there had to be a designer that designed the facial recognition software that articulated points on the face in order to conduct the searches in the first place, and databases had to be established by designers in computer systems to link these pictures. Without databases, faces cannot be recognized. Comparisons have to be made between faces, and depending on the breadth of the database, this will limit or stretch the possibilities of identification. For instance, a small town in rural Arizona with a database of only those in the county would have less potential for finding a match if the database was not linked up to a larger system like those controlled by the FBI. Both the programming of the computer's ability to recognize faces and also the database itself would face technological limitations.

In the case of this dissertation and the texts on BI reform, technology plays an important role in gathering data and maintaining databases on those who have clearances. It also helps sort those who will get clearances with those who will not. It also helps explain the way current

surveillance practices are carried out. For an example, Representative Stephen Lynch commented that the crafting of legislation for BI improvement, and specifically the Security Clearance and Reform act of 2014, must lay out ways to streamline and eliminate outdated manual processes “in favor of electronic and accessible investigative databases” (*DC Navy Yard Shooting: Fixing the Security Clearance Process*, 2014, p. 148). This example not only expresses the preference for technology, but it also implies that technology will be better than a manual process and will increase the value of BIs. Keeping in mind the subjectivity of technological filtering though, we see that these databases are not impartial and are created using institutionally-biased criteria.

Background Investigations

Now that some of the basics of rhetoric and surveillance have been detailed, it is also beneficial to understand, at least in an abridged way, how the Federal BI process works. Regardless of what level of security clearance one gets though, there are six steps which underlie the BI process (*The Navy Yard Tragedy*, 2013). While each level may warrant additional steps, there is a basic underlying method. Figure 2 details this process.

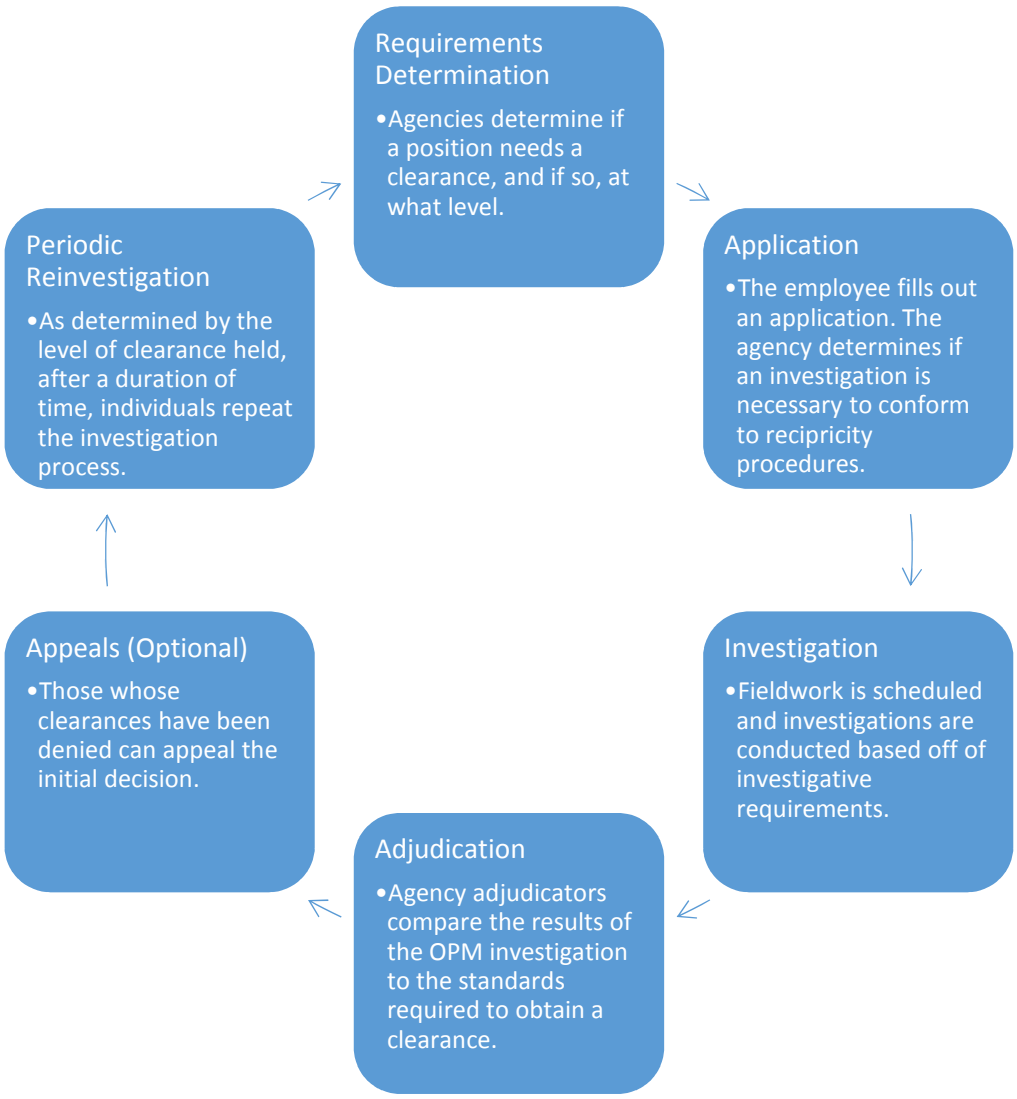

Figure 2. Steps of the BI. Note: Data from *The Navy Yard Tragedy* (2013).

As shown in Figure 2, first, an agency must determine that an individual's position needs a security clearance, and this discretion is left up to the agency which employs the individual that needs a clearance (*Safeguarding Our Nation's Secrets: Examining the Security Clearance Process*, 2013). The agency head looks at the activities that the position conducts and assigns a subsequent level of sensitivity. This also shows that clearances then are attached to a certain position and not the people in particular (*The Navy Yard Tragedy*, 2013). If an agency thinks a position affords access to elements of national security, then the person will need a clearance. If

that person quits the position, then the person will no longer need that clearance. The job, not the person, warrants the BI.

Second, after it is determined what level of clearance is needed, an individual then fills out the appropriate paperwork. BIs start with a requirement to complete the appropriate form (e.g., SF-85, SF-85P, AND SF-86) which depends on sensitivity, risk, and security clearance access (*The Navy Yard Tragedy*, 2013). The forms ask for similar but increasingly more complex information depending on the level of clearance. The SF-86 is the most complex form asking for information "about residences, employments, military service, education, spouse, relatives, and associates . . . mental health, criminal activity, drug/alcohol use, credit, and allegiance to the United States" (Maryland.gov, n.d.).

Based on the answers on these forms, the field investigative work is conducted. For the majority of security clearances, the fieldwork is conducted by OPM's FIS division. According to Congress, over 90% of BIs for the federal government are conducted by OPM[31] including all background including all Department of Defense members, civilians, and contractors (*Safeguarding Our Nation's Secrets: Examining the Security Clearance Process*, 2013, p. 2). There are other agencies such as the FBI who conduct their own investigations for those such as "[h]igh level Presidential appointees, cabinet officers, agency heads and staff who may work at the White House directly for the President" (USOPM. "Frequently Asked Questions," n.d.), but otherwise, OPM conducts the investigations for the majority of federal agencies.

In addition to standard automated checks, depending on the particular investigation conducted (see Figure 3), the data listed on the forms by the Subject of investigation initially guides the investigative field work process. Investigators combine the answers provided on the questionnaires and the testimony they receive from the sources with whom they interact in order to construct a report on the subject of investigation. Michael Rhodes, Executive Vice President at CACI describes this process as fact-finding through the requirements of handbook investigative

[31] As a caveat, and as discussed in the surveiller's section, federal employees for OPM do not conduct the majority of their investigations. In the 1990s, the Clinton Administration outsourced much of OPM's investigative work (*DC Navy Yard Shooting,* 2014), and by 2014, 70% of OPM's investigations were conducted by contractors (H.Rep, 2014; *DC Navy Yard Shooting,* 2014).

standards (*DC Navy Yard Shooting*, 2013), and the Government Accountability Office adds it is also a corroboration of the subject's provided information (*The Insider Threat to Homeland Security*, 2013). Cooperation by those interviewed on behalf of a subject of investigation is voluntary, and in order to complete the investigation, investigators must find best sources which cover the activities listed on the forms (*Safeguarding our Nation's Secrets: Examining the Security Clearance Process*, 2013). For some investigations, the contact is predominantly through written or computerized inquiry, and for others, there may be a significant amount of fieldwork conducted in person (Maryland.gov, n.d.; *The Navy Yard Tragedy*, 2013). The completion time depends on the level of investigation, and the higher the clearance, the longer the investigation will potentially be. For instance, a top secret clearance is more in-depth and "requires 10 times as many investigative staff hours as a secret clearance" (S. 113-276, 2014).

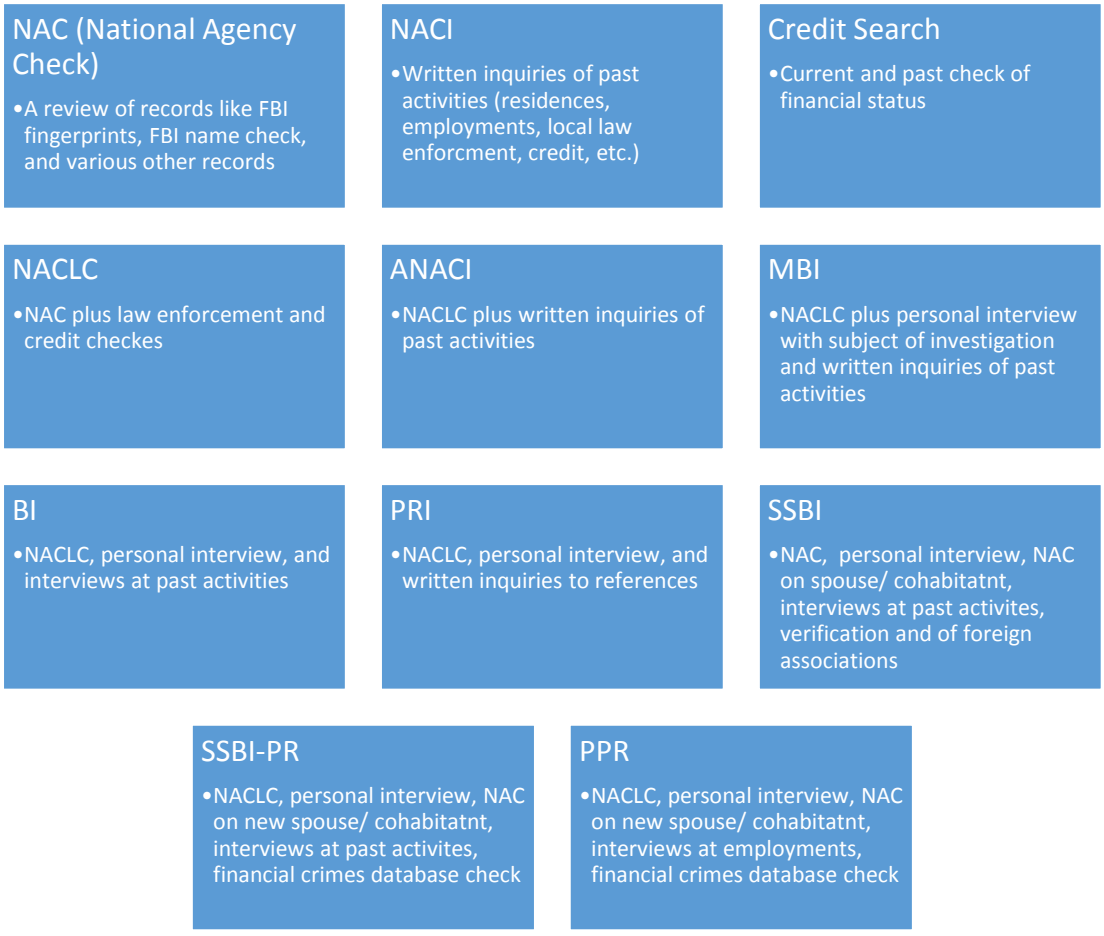

Figure 3. Investigations Description. Note: Data from Federal Clearance Assistance Service, n.d.

After the BI is conducted, this information is turned over to the agency that ordered the investigation, and this agency makes the determination as to whether the individual should have that clearance (*Safeguarding our Nation's Secrets: Examining the Security Clearance Process*, 2013, p. 9). Thus, the third process then is adjudications. In the adjudication phase, adjudicators review the investigation to determine if the individual is suitable for a clearance. The current adjudicative process is based on White House guidelines issued in 2005 (*The Navy Yard Tragedy*, 2013). Figure 4 provides the criteria for adjudications.

Allegiance to US
Foreign influence
Foreign preference
Sexual behavior
Personal conduct (like falsifying the security questionnaire)
Financial history
Use of alcohol
Use of drugs
Mental and emotional health
Criminal history
Security violations
Outside activities like foreign employment
Misuse of IT

Figure 4. Adjudications Criteria. Note: Data from USGAO (2013)

Of interest to note, OPM does not adjudicate other agencies' BIs. A BI is like a product for OPM, and other agencies will order the appropriate BI based on the assessed position designation. Unless the person under investigation is planning to work for OPM, then OPM will not be involved

in the adjudicative process. Adjudicators are located within the agency that ordered and purchased the BI from OPM.

The final step in the BI process is the reinvestigation. This step occurs after the original investigation has been granted and time has elapsed. Depending on the type of investigation the individual went through and their current clearance needs, an individual undergoes an additional investigation that will update the BI and note any changes that have occurred since the last investigation. For two common types of investigations, the standards for TS clearance require a reinvestigation every five years, and standards require a reinvestigation every ten years for Secret clearances (USGAO, 2013; *The Navy Yard Tragedy*, 2013).

Another portion of the cycle is the appeal. Individuals are also allowed a chance to appeal their investigation if denied a clearance. The process is different depending on agency, and not everyone would need to to appeal their determination (*The Navy Yard Tragedy*, 2013). This step is built into investigation process though, and it remains a step that can be utilized if necessary.

Conclusion

Overall, these conversations of rhetoric, surveillance studies, and BIs are designed to ground my research. I initially looked at the rhetoric of the congressional documents for the rhetoric of what they were saying without attempting to use a filter to see what terministic screens Congress was using. I then applied the terministic screen of surveillance studies by focusing on eight specific themes of this field to see another perspective for the documents. The overall discussions revealed that the application is overlooked and the BI is taken for granted. Both conclusions will be discussed in chapter five.

Since I'm using the idea of the terministic screen though, I want to extend the conversation a little more. By using rhetoric to look at the argument in terms of what is being said, I acknowledge that I am using my own terministic screen to read the congressional documents. I will be making the assumption that I am providing one explanation of causes and solutions. But as Burke brought out, "Every way of seeing is also a way of not seeing" (Burke, 1984, p. 70), so I also want to explore another path of seeing. One way to see what is not being said in my

explanation is to looking outside of one terministic screen is to apply another screen to the discussion. According to Burke (1966/1990), “[A]ll scientific terminologies, but by their very role in specialized disciplines, are designed to focus attention upon one or another field of observation” (p. 1039). Thus, to see outside of one screen, one could apply another screen for analysis.

CHAPTER 3

METHODOLOGY

In simple terms, qualitative research is a collection of methods which can be described as a “situated activity that locates the observer in the world” (Denzin & Lincoln, 2005, p.3) and “consists of a set of interpretive, material practices that make the world visible.” It is a way to look at any type of information that can be considered data and turn it into something able to be interpreted. It encompasses many different genres of analysis like ethnography, grounded theory, phenomenology, and case studies, and it seeks to analyze information that may be harder to quantify such as interviews, field notes, or photographs that document social action about oneself or others (Bos & Tarnai, 1999; Denzin & Lincoln, 2005; Saldana, 2011). It attempts to view the world through a more natural setting and tries to make sense of meanings that people place on activities (Denzin & Lincoln, 2005).

For this study, I used the qualitative method of content analysis. Content analysis is an empirical way to systematically analyze texts, be it transcripts, images, speeches, film, artifacts, etc. (Bos and Tarnai, 1999; Mayring, 2000; Saldana, 2011). According to Elo and Kyngas (2007), the general goal of content analysis is to get a “condensed and broad description of the phenomenon, and the outcome of the analysis is concepts or categories describing the phenomenon. Usually the purpose of those concepts or categories is to build up a model, conceptual system, conceptual map or categories” (p. 108). It works to turn a body of information into knowledge by identifying patterns which emerge when looking at data.

Scholars break down application of the process of content analysis in different ways, but there are fundamental phases that underlie differing procedures for this process. Condensing recommendations, there are six essential steps to the process. These processes are:

1) The researcher decides what needs to be analyzed and selects relevant texts.
2) The researcher becomes familiar with the texts.
3) The researcher constructs a scaffold though which to sort and code the material.
4) Before finalizing the scaffolding, the researcher conducts a pilot study.
5) The researcher then conducts the study and codes the material using the scaffolding.

6) The researcher then draws conclusions and details the processes he/she used to conduct the study.

A brief synopsis of each step will help to understand these processes in more detail.

Step One – Analyzing Relevant Texts

In the first phase of content analysis, a researcher decides what is going to be analyzed. Elo and Kyngas (2007) call this the preparation phase. According to Mayring (2000), in this step, a researcher should start to select a unit of analysis, be it a word or theme,[32] for the overall study. Questions should be considered such as: what texts should be analyzed? Will only the text be considered? Should the delivery of the text be analyzed? Will the context be examined? A researcher must also decide how much material should be examined (Schreier, 2014). While it is important to selectively limit how much material to be analyzed, it is important that the pieces that are chosen are relevant and influential enough to be meaningful. As Elo and Kyngas (2007) add, "[T]he sample must be representative of the universe from which it is drawn" (p. 109).

My study began at this step. Because a qualitative content analysis study is closely intertwined with the research questions,[33] I needed to define my questions first which were: based on congressional hearings, bills, daily editions, and reports/publications, since Congress began to react to Snowden's disclosures in June 2013, what arguments have emerged in the documents as flaws in the BI process? And how does applying another terministic screen change the interpretation of the congressional communication?

I chose these questions because, as discussed in chapter one, I was interested in the congressional discussion resulting from the actions of both Snowden and Alexis, especially in the larger context of BIs and their use for security clearances. After establishing these questions, I chose to limit the texts to congressional documents because these types of documents are the primary sources of information distributed by the institutions that I wanted to study; Congress is

[32]A *word* connotes the basic element of speech, and Bos and Tarnai (1999) define *theme* as "single assertion about some subject" and one of the most useful elements of content analysis (p. 647).

[33] The research questions help define the unit of analysis (for instance, post-Snowden BIs).

the law making branch of government, so they determine institutional rules that would outline what is needed for reform.

The literature then suggests that the researcher starts with a unit of analysis, determines how much material should be analyzed, and makes sure the materials are representative of the universe from which they were drawn. In order to complete these steps, I used the Arizona State University library search tool *One Search*. I chose to focus on filtering through specific words so that the content of the documents would address the research questions I was trying to answer. I chose to search the Boolean phrase "(U.S. Congress) AND ("background investigations") AND ("security clearance process")." I selected those keywords because I wanted to see what Congress had to say about security clearances for background investigations. After entering these search terms, I selected only "government" documents published from June 2013 to July 2015 (time of data gathering) in order to limit the documents to material published by the government since Snowden began divulging information. I did this in order to research Congress' reforms in a post-Snowden environment. This compilation of documents worked best for my study because after doing a cursory analysis of the documents, they explained what background investigations are and what current problems exit since Snowden.

By doing this search, I originally came up with twenty-nine articles about the subject which fit into four categories: congressional hearings, bills, daily editions, and reports/publications. Table 1 provides a sample view of four of those documents. Appendix S offers a complete list of the documents under review and their corresponding document number.

Table 1.

Types of Documents in the Study

	Hearing	Daily Edition	Bill	Report/Publication
Example	"DC Navy Yard Shooting: Fixing the Security Clearance Process" (*DC Navy Yard Shooting*, 2014)	"OPM IG Act H.R. 2860." (113th Cong. Rec. H.R. 2860, 2014)	"Security Clearance Reform Act of 2015" (H.R. 490, 2015)	"Information Security: Agencies Need to Improve Oversight of Contractor Controls" (USGAO, 2014)

Of the twenty-nine articles that come up in the results, there were issues accessing five of the articles directly from the ASU search site. Because of these access issues, four (articles 10, 18, 21, and 29) of the twenty-nine articles were not included in the study. These four were excluded because they appeared to be duplicates of other articles because they had the same titles. Articles 10, 11, and 21 had the same title of "Security Clearance Accountability, Reform and Enhancement Act. Congressional Report. Congressional Report." Also, articles 18 and 19 were called "Preventing Conflicts of Interest with Contractors Act," and 26 and 29 were called "Enhanced Security Clearance Act of 2014. Congressional Report. Congressional Report." Because article 11 was able to be opened but 10 and 21 could not be, I could not tell if there was a difference between articles 10, 11 and 21. Similarly, this was also the case with article 18 and 19 and with articles 26 and 29. The fifth article, article 13, would not open through the database; however, this article could be located through a web search of its name "House Consideration and Passage of H.R. 2860. Congressional Record Daily Edition Excerpt" (OPM IG Act, 2014). Since there were no articles with an identical title occurring elsewhere on this list, I included this article in the study as there was not a concern it was a duplicate.

Step Two – Become Familiar with the Texts

The second step of the content analysis process involved getting familiar with data and then estimating what categories might work for the data. Mayring (2000) considers this as one of the basic ideas of content analysis (specifically, part of his *rules for analysis*), and Elo and Kyngas (2007) call it the "organizing phase." This step of the process involves getting familiar with the chosen material, examining it, and then deciding how to create a step-by-step process for categorizing the data through codes (Mayring, 2000). Additionally, only reading the documents once isn't enough; a researcher needs to be very familiar with the documents before conducting this step-by-step process. According to Elo and Kyngas (2007), "The aim is to become immersed in the data, which is why the written material is read through several times…[and] no insights or theories can spring forth from the data without the researcher becoming completely familiar with them" (p. 109). A researcher needs to understand what is being presented and then adapt a

review process built upon their multiple readings because the next step of scaffolding can't be done without knowledge of what the texts say.

For my study, in order to carry out these steps, I first did a thorough read of the documents from approximately three hundred hours (twenty-five hours per week from July to September 2015) before attempting to build or solidify the final scaffolding that I would use for my dissertation. This initial reading allowed me to understand what the documents said as individual pieces and as a more comprehensive collection of materials. In order to keep track of this information, I complied a spreadsheet of passages that represented the emerging categories, kept track of the document number,[34] identified the title of the document, listed the type of a document, and kept track of the publication date of the document. I also attempted to assess a manifest meaning[35] by making a general description of the document and latent meaning by identifying underlying values in the document. I also wrote down any questions that came up, and I wrote down keywords in a "general" category that I felt represented the document on a whole.

Step Three – Construct a Scaffold

After becoming familiar with the data then, the next step was to use the organizational planning from the previous step but to now frame and construct scaffolding through which to sort through the available material. As described in step two, I had my spreadsheet of data composed for the last step, but for this step I moved to make specific categories for coding the documents. Schreier (2014) calls this structuring and says it "refers to creating the main categories and generating to creating the subcategories for each main category" (p. 176). Mayring (2000) discusses this step under his "Categories in the Center of Analysis" section, and Elo and Kyngas (2007) include the next actions as being in the second, organizing stage. Put simply, according to Mayring (2000) this phase involves determining the rules, followed by the questions, to help put the material into categories which are continuously revised through feedback loops. The

[34] The document number is a number I assigned as a result of the ASU One Search tool. The document number was assigned to the document based on where the document resulted in the search. There was no additional significance placed on this number to include date or type of publication.

[35] The difference between manifest and latent meanings are listed in a section below.

researcher must decide the best way to categorize and sort through the possibly overwhelming amount of data. The rules are not arbitrary either, and they must be calibrated to match the overall method and purpose of the design. This process is a very important step, and according to Schreier (2014), “This frame is at the heart of the method, and it contains all those aspects that feature in the description and interpretation” (p. 171). Schreier continues, “[M]ain categories should cover one aspect of the material only…Second, subcategories within one main category should be created so that they are mutually exclusive... [and] all relevant aspects of the material must be covered by a category (requirement of *exhaustiveness)*” (p. 175).

To carry out this step for my dissertation, I started with the question: based on congressional hearings, bills, daily editions and reports, since Congress began to react to Snowden’s disclosures in June 2013, what arguments have emerged in the documents as flaws to the BI process, because that question constrained my analysis of texts. I used this as the main category and called it “Federal BI Flaws.” I further subcategorized any passage that I found in the texts that I thought illustrated the idea of a flawed BI. These subcategories were developed when patterns emerged through multiple readings of the documents. By then end of the study, there were approximately thirty-eight different subcategories that the data was entered into as show in the chart below in alphabetical order. Table 2 details these subcategories.

Table 2.

Flaws of the BI process that Emerged from the Documents

Federal BI Flaws – Alphabetical Order		
• Adjudication • Amount of classified info • Audits • Communication (lack) • Contractors • Facilities • Finances • Forms • Fraud • General questions	• Historical precedence-studies • Incomplete investigations • Internet/social media • Law enforcement • Legislation - current • Mental health • Metrics • More/continuous evaluation • National security state • Oversight/review • Prediction • Position designation/# of clearances	• Process • Quality • Reciprocity • Reports - Need more • Revocation/ suspension/appeals • Safeguard for employees • Self-reporting • Speed, efficiency, timeliness • Standardization • Tax debts/debts

• Historical precedence-events		• Technology • Time between investigations • Training • Transparency • USIS

In the analysis, the thirty-eight categories were grouped into eight more condensed categories which allowed for an easier analysis of the results. The results for the most part aligned themselves with the steps of the BI process except for the categories of a general discontent with the overall process of the BI (and not particularly one step) and a category of oversight which discusses surveilling the surveillance. The groups are grouped into the larger categories as detailed in Table 3.

Table 3.

Flaws in the Federal BI Process

Federal Flaws - Groups			
Overall Process: • Communication (lack) • Finances • General questions • Historical precedence-studies • Historical precedence - events • Legislation - current • Prediction • Process • Self-reporting • Speed, efficiency, timeliness • Standardization • Technology	**Oversight** • Audits • Metrics • Oversight/ review • Quality • Reports – Need more • Training • Transparency	**Requirements Determination** • Amount of classified info • Position designation/# of clearances • Facilities • National security state	**Application** • Forms • Reciprocity
Investigation • Contractors • Fraud • Incomplete investigations • Internet/social media	**Adjudication** • Adjudication	**Appeals** • Revocation/ suspension/ appeals • Safeguard for employees	**Periodic Reinvestigation** • More/ continuous evaluation

• Law enforcement • Mental health • Tax debts/debts • USIS			• Time between investigations

Each of these categories were used to sort the information after they emerged as patterns. Additionally, each category could further be reduced by subcategory, and these further reductions will be discussed in chapter four. Sample textual passages are included in Appendix J-Q.

Additionally, there is a miscellaneous category which kept track of data that didn't fit into a category based on the research questions but did seem important for future research. The passages in this document either provide background information about specific stakeholders or processes outside of the research questions or examined themes not directly looked for through the lens of the research questions. For instance, the topic of "OPM's Role" details what role OPM plays in the investigations in a more factual matter (e.g., OPM conducts 90% of the investigations) rather than discuss OPM's role in the problems of BIs, and the section "Trust" includes passages implying there is a trust of the BI system. The idea of trust is outside of the research questions aimed at finding what was wrong with the BI process and instead looks at what is right and what is trustworthy. Because this was miscellaneous category, the information was not as detailed as the rest of the data and is arranged as shown in Appendix C by article number rather than further reduction of the subcategories. The contents of this section are detailed in Table 4.

Table 4.

Miscellaneous Results

Background Information	Miscellaneous Themes
• Costs • Definitions • OPM's Role • Physical security • Steps of a clearance process • USIS • What clearances do • Who has a clearance	• Feelings about the BI • General distrust of BIs • Liberties/Freedom • Privacy • Trust • Whistleblower

Manifest or Latent

Inside this step are several additional important things to consider. One factor is that in order for the researcher to look at the texts and determine categories and subcategories, the researcher must decide if they are attending to manifest content, latent content, or both. A manifest meaning is the content of what the text says on the surface and includes what is visible to the observer (Graneheim & Lundman, 2004; Saldana, 2011). On the other hand, a latent meaning is "one that is suggestive, connotative, and subtextual" (Saldana, 2011, p. 10), a contextual analysis (Mayring, 2000), an analysis of the larger scope of what the text is talking about in relationship to other texts and ideas, or involves interpreting underlying meanings of the text (Graneheim and Lundman, 2004; Hsieh & Shannon, 2005). Depending on the format of the texts too, this could be the physical conditions existing around the texts and their delivery (Elo & Kyngas, 2007). For instance, according to Elo and Kyngas, (2007), "The aim with latent content is also to notice silence, sighs, laughter, posture etc." (p. 109). This information though would not necessarily be available for those reading written texts (as in a more traditional definition of the written word). Overall though, depending on the goal of the researcher and the researcher's study, the researcher would need to decide whether manifest, latent, or a mixture of the two will be used, and whether this information was pertinent to the research questions posed.

For this dissertation, in the study in particular, I focused only on the manifest content of the text (or what was on the surface and what was visible to me) for the coding and scaffolding. I did this because during the preliminary readings when I attempted to record latent content, I did not feel adequately able to assess this content type. There were no physical contextual cues outlined in the documents, and I did not want to assume that I understood underlying meanings of the texts outside of what they presented on the surface. However, when I wrote up the results of the study in chapter five, I did draw conclusions based on the results of the study, but I did this through the lens or terministic screen of surveillance studies.

Inductive or Deductive

The second major choice a researcher needs to consider, and one that would have a major impact on the way the study is designed, is whether they will be using an inductive or deductive method (Elo & Kyngas, 2007; Mayring, 2000). As a general overview, for an inductive content analysis, "the concepts are derived from the data" (Elo & Kyngas, 2007, p. 107). On the other hand, "[d]eductive content analysis is used when the structure of analysis is operationalized on the basis of previous knowledge." This means that inductive content analysis is more about the categories that spring up from the text during the readings/analysis as related to the research question, and deductive content analysis uses the text but also incorporates some outside theory from the start of the initial coding. Elo and Kyngas (2007) further make the differentiation between the two categories by outlining, "An approach based on inductive data moves from the specific to the general, so that particular instances are observed and then combined into a larger whole or general statement" while "[a] deductive approach is based on an earlier theory or model and therefore it moves from the general to the specific" (p. 109). Depending on the researchers' choices of process, the data will be gathered in different ways.

Breaking down the processes, according to Mayring (2000), the first procedure in the inductive method is to conduct is *inductive category development*. According to Mayring, this means that one should:

> … [F]ormulate a criterion of definition, derived from theoretical background and research question, which determines the aspects of the textual material taken into account. Following this criterion the material is worked through and categories are tentative and step by step deduced. Within a feedback loop those categories are revised, eventually reduced to main categories and checked in respect to their reliability. (n.p.)

In this type of method, the researcher does not start with a prearranged idea of what they will be looking for. Schreier (2014) calls this a data-driven method, and researchers begin to look at the data and attribute codes to it based on patterns that start emerging from the content itself. Elo and Kyngas (2007) describe this as open coding or creating categories and abstraction. The authors state, "Open coding means that notes and headings are written in the text while reading it. The written material is read through again, and as many headings as necessary are written down in the margins to describe all aspects of the content" (p. 109). This information is then

placed in categories which will “provide a means of describing the phenomenon” for more clarity and knowledge generation” (p. 110).

As this material continues to be reread, as described above, the categories and coding gets revised after continuing to go back over the material (Mayring, 2000). Elo and Kyngas (2007) add to this and state, “After this open coding, the lists of categories are grouped under higher order headings” which decreases categories “by collapsing those that are similar or dissimilar into broader higher order categories” (p. 110). According to Schreier (2014), the coding process in a data-driven study will look like this:

1. Reading the material until a relevant concept is encountered.
2. Checking whether a subcategory that covers this concept has already been created.
3. If so, mentally ‘subsuming’ this under the respective subcategory.
4. If not, creating a new subcategory that covers this concept.
5. Continuing to read until the next relevant concept/ passage is encountered.

> This process is continued until a point of *saturation* is reached; that is, until no additional new concepts can be found. (p. 176)

Mayring (2000) provides the following diagram of this method in Figure 5.

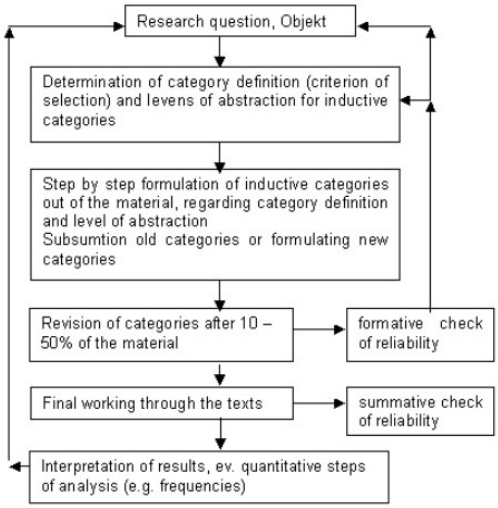

Figure 5. *Inductive category development.* Note: Data from Mayring (2000) under a creative commons license and retrieved from http://www.qualitative-research.net/index.php/fqs/%20article/view/1089/2385.

The second method is the *deductive category application.* Schreier (2014) refers to this a concept-driven method, and according to Elo and Kyngas (2007), deductive content analysis relies more on previous theories and models, and "is used when the structure of analysis is operationalized on the basis of previous knowledge and the purpose of the study is theory testing" (p. 109). The deductive method then starts with more structure and uses the coding to build on preexisting knowledge. The main idea here is to give explicit definitions, examples and coding rules for each deductive category, determining exactly under what circumstances a text passage can be coded with a category (Mayring, 2000). After deciding on the use of the deductive method, the next step is to develop a matrix which helps code the data into categories (Elo & Kyngas, 2007). When this is created, only the relevant data that fits under the categories is added included in the study. Otherwise, the data can still be used but becomes unstructured and moves towards the inductive method which allows for open coding. Figure 6 illustrates Mayring's idea of the deductive method. Figure 7 provides one section of a chart illustrating a matrix application of these steps.

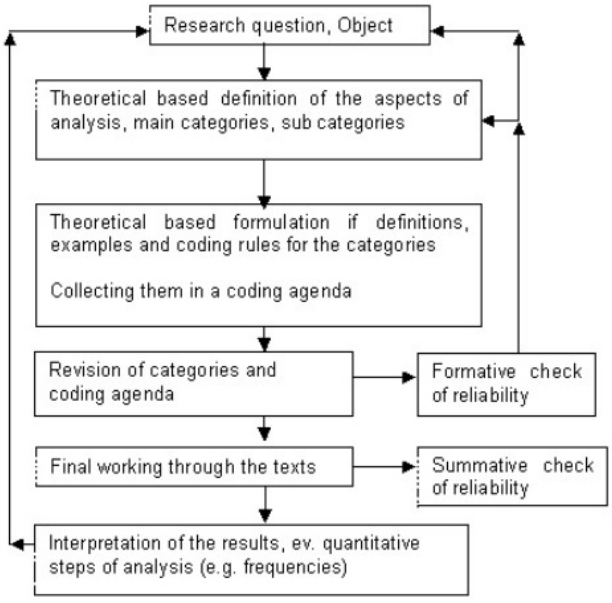

Figure 6. Deductive Category Application. Note: Data from Mayring (2000) under a creative commons license and retrieved from http://www.qualitative-research.net/index.php/fqs/%20article/view/1089/2385.

Category	Definition	Examples	Coding Rules
C1: high self confidence	High subjective conviction to have successfully coped with the situational demands, which means - to be clear about the demands and their coping possibilities, - to have a positive, hopeful feeling in handling the situation, - to be sure to have coped with the demands on ones own efforts.	"Of course there had been some little problems, but we solved them all, either I myself or the student gave in, depends who made a mistake. Everyone can make mistakes." (17, 23) "Sure there had been problems, but in the end we had a fine relationship. We got it all together." (27, 33)	All three aspects of thew definition have to point to "high" self confidence no aspect only "middle" Otherwise C2: middle self confidence

Figure 7. Application of Deductive Category. Note: Data from Mayring (2000) under a creative commons license and retrieved from http://www.qualitative-research.net/index.php/fqs/%20article/view/1089/2385.

According to the Schreier (2014), “Category names should provide concise descriptions of what a category refers to” (p. 176). Descriptions on the other hand should provide “what is meant by a given category and what features are characteristic of the category” (p. 176). An example provides textual evidence as to what the category and definitions mean, and the coding rule establishes what must be considered before including a particular unit into the category. Each element should be present in the deductive method so that continuity can be achieved to the greatest extent.

For my study, after doing this preliminary research, I came to the conclusion that, due to the nature of the research questions, I would collect data using both inductive and deductive methods. I took an inductive approach so that I could code the material openly based on the first research question. I wanted to know what the texts suggested were flaws, and since, as discussed, the main idea of inductive procedures is to formulate a criterion of definition based off the text, the inductive approach worked best to answer this question.

To gather the information, after reading each passage, I recorded relevant sentences that represented the paragraph or passages surrounding them. I did not take every sentence, but I

recorded a representative selection from each passage that represented or formed a specific theme. For instance, in a paragraph discussing that investigators don't use the internet, I recorded "Currently, investigators do not review subjects' social media or traditional media records. Those sources of information should be reviewed in appropriate circumstances to conduct more thorough investigations" (*DC Navy Yard Shooting*, 2014, p. 34) because this sentence summarized the general sentiment of the whole unit of thought. If a representative sentence was not available, I summarized the data without direct quotes. For instance, I summarized a passage in *The Navy Yard Tragedy* (2013) as "records for law enforcement, health, and financial data need to be more accessible."

For the second question asking about applying another terministic screen to the interpretation of the congressional communication, I used the deductive method. As stated in chapter one and two, I applied eight lenses (constancy, surveillant assemblage, surveillers, sorting, risk, prediction, identity, and technology) to the texts in order to first identify that BIs were surveillance, and then to use surveillance to look at the conclusions through a terministic screen. In this way then, these lenses provided previous knowledge of a theory to the Congressional documents. Instead of the inductive method which looked at what was presented and then let the categories emerge, this method started with the categories and looked at how the texts fit into these categories. I recorded the passages for this question in the same way as I did in the first question as described above. The data was arranged by Category >Definition>Examples>Coding Rules. Table 5 provides an example of this method for prediction, just one of the eight lenses. Sample textual passages are included in the appendix.

Table 5.

Deductive Example – Prediction

Category: Prediction
Definition A main purpose of surveillance technologies is to be proactive or predict the future (Gates, 2011; Graham & Wood, 2003; Jewkes, 2004; Kim, 2004)

Coding Rules
• Use of tech to predict the future • Specific technological programs
Examples
More technological monitoring = prediction • "Timely knowledge [through technology] of such information [damage assessments regarding individuals involved in unauthorized disclosures of Classified information or acts of workplace violence] might have prompted a security review or increased monitoring of that individual" (*The Insider Threat to Homeland* Security, 2013, p. 17). • "One potential element of the Insider Threat Program is the use of analytics to identify and even predict potential breaches of information systems based on an individual's pattern of system access" (*The Insider Threat to Homeland* Security, 2013, p. 49). • "In the interim, the Department has held discussions with private firms that look at behavioral modeling through continuous evaluation to explore automated options and their availability/ compatibility with current systems" (*The Insider Threat to Homeland* Security, 2013, p. 49). • "For example, the Identity Management Enterprise Services Architecture (IMESA) was identified as a potential capability to continuously monitor personnel that have authorized access to DoD installations and assets against authoritative data sources. IMESA will enable the sharing of identity and physical access control information complementing on-going continuous evaluation concept demonstration efforts" (*The Insider Threat to Homeland* Security, 2013, p. 49). • "Additionally, under a continuous re-evaluation system, Alexis' two visits to VA emergency rooms in August 2013 could have been immediately flagged" (H. Rep, 2014, p. 11)

As seen in the example above, I took a category, defined it, created coding rules, and then provided textual examples which illustrated the definition and coding rules. Each example passage provides examples of how technology is used to try to predict the future in BIs. For instance, IMESA hopes to share information so that risky behavior can flag potential adverse behavior, and this in turn will hopefully prevent any adverse actions. Table 6 below provides an abridged summary of the full results of each category.

Table 6.

Surveillance Results

Surveillance Rhetoric	
Constancy	**Surveillant Assemblage**
• Continuous assessment o Definition	• Expanded collection, agency, and scrutiny

o Drawbacks/ Limitations o Frequency o Gap between investigations o History o How it works o Programs o Real time o Role of Tech o Why used/ justification- generic examples o Why used – specific examples	o Multiple sources of information • Multiple locations o Locations • Power not limited to place o Reciprocity
Surveillers • Different surveillant agents o Contractors o Employees	**Sorting** • Databases o Adjudication o Difference between crimes o Sorting as tool for acceptance/denial o Tech • Codes o Facilities o Law enforcement • Consumer surveillance o Credit Use
Risk • Types of risks o Adjudicative guidelines o Alcohol o Association o BIs o Can't get all o Communication o CE o Contractors o Credit o Damage potential o Derogatory info o Documents missing o Drugs o Education o Employment o Facilities o Foreign o Inside threats o Internet o Law enforcement o Lifestyle o Mental / emotional o Prohibited items o Residence o Sources o Subjects o Terrorism	**Prediction** • How to predict o Alert o Continuous evaluation o Credit o More people, more risk o Processes o Random o Warning Signs/ Flagging/ High Risk Designations • Technology and Prediction o More technological monitoring = prediction • Probabilities and Prediction o Belief in prediction o No belief in prediction o Only past account – skeptic

o Under-reporting • Risk communication systems o Adjudication o Director of National Intelligence (DNI) o Determination of clearance o Facilities o Investigator o Level o OPM o Problems o Reciprocity o Rules, regulations, laws o Steps of a clearance • Basis for assessment o Access to food supply o Adjudications decide suitability o Alcohol o Citizenship o Conduct o Dishonesty is bad o Drugs o Employment problems o Financial problems o High-risk individuals o Law enforcement o Mental health o Need identity	
Identity • Articulated in context o Adjudications o Changeable o People don't agree with determination o Whole person • Obsessed with checking IDs o Facts Exist o ID Card o ID Cards revoked for derogatory info • Ascribed by institutions o Government-defined identities o Identity based on adjudication • Biometric ID o Fingerprints o ID • IDs are self-generated and revealed information o Public info and social media o Self-reporting o SSNs • Basis for assessment (also in risk) o Access to food supply o Alcohol o Adjudications o Citizenship	**Technology** • BIs using tech o Accuracy o Automation o Collection o Continuous evaluation o Control o Cost o Database o Delivery o Duplication o Enterprise-wide /database o Exclusion o Internet/social media o Paper o Programs o Reliability o Sharing o Solution o Tools o Unrealistic o Web-based • Tech and biometrics o Automation o Continuous evaluation o Database

o Conduct o Dishonesty o Drugs o Employment o Financial problems o High-risk individuals (also in prediction) o Law enforcement o Mental health o Need firm identity	o Enterprise o Fingerprints o Program • Confinement and exclusion o Keeping in / keep out • Everyday use of tech o Public and social media

Step Four – Conduct a Pilot Study

Before doing the actual study, it is important to conduct a pilot study to evaluate the fit of the structure and coding before finalizing the process. Coding and categorization need to be uniform in the study, and the study needs to be consistent. Any problems with the scaffolding should be worked out before the study because consistency of application is important to the overall process. A series of steps should continually be followed when doing this coding (Graneheim & Lundman, 2004; Hsieh & Shannon, 2005; Mayring, 2014; Schreier, 2014). Schreier (2014) recommends, "Once all categories have been generated and defined, it is time to take a step back, look at the structure of the coding frame once again, and 'tidy up' any loose ends. If subcategories are very similar, it might be best to collapse them" (p. 177). A pilot study should thus ensure that the processes will work and achieve desirable results.

Before conducting my actual study, in addition to assessing the information during my initial read-through, I composed a pilot study of the more solidified coding because, as the literature suggested, the scaffolding should be consistent once the final analysis is underway. In this pilot study, I assessed the first five selected texts and tested whether my categories would hold up and fit with my selected scaffolding and coding. I was satisfied with my results and continued to code accordingly. The final coding incorporates the pilot study because the pilot categories adequately fit the texts.

Step Five – Conduct the Study

After doing a pilot study, conducting the actual study is the next step of the process. After the information has been evaluated, and when a researcher has figured out what type of framework and organization will be used, the researcher can then conduct the study based on the structures he or she set up. The researcher will follow the framework set up and sort through and

code the data accordingly. This outcome of this coding will make the study transparent and provide the data for the researcher.

For my study, after the coding choices were made, I set up my coding scaffolding and did the coding. As the literature advised, for the inductive coding, I set up a very open system to categorize the data to help answer the first questions. For the deductive analysis for the second question, I set up eight categories based on pre-existing surveillance knowledge from the field of surveillance studies: constancy, surveillant assemblage, surveillers, social sorting, risk, prediction, identity, and technology. For the first question, I went through the texts and recorded passages representing the post-Snowden BI flaws. As discussed earlier, the texts fit under the categories of "Federal BI Flaws" and "General BI Flaws," and I set up in a chart similar to the deductive method. I do not consider them deductive though, as the categorization was not based on theory or additional knowledge; the categories grew from the data itself. The first category in which I defined "Federal BI Flaws," and I said the coding rules required everything that was included should support the idea that there is an overall "challenge to BIs as being currently flawed and fixable." For the second category, "General BI Flaws," I said the definition is the belief that BI principals and assumptions are fundamentally flawed or not as safe as it seems, and the coding rules were texts that challenge to BIs and its associated assumptions as flawed or problematic beyond post-Snowden issues. Eventually, these categories were subcategorized into the eight Federal Flaws groups as shown in Table 3.

The previous section detailed the emergent categories of each main category. However, the below example provides an example of what those subcategories look like. For instance, two subcategories (and the first two subcategories) for this section are "adjudications" and "amount of classified information." Under each category, textual evidence is given that supports that BIs are flawed, need to be fixed, and that adjudications or amount of classified information are involved. Table 7 illustrates this.

Table 7.

Inductive Results Example – Federal BI Flaws

Subcategory	Textual Examples
Adjudications	"…do you think any improvements are needed on the adjudicative end as to what standards should be used, what thresholds there should be? Ms. Farrell. Our work is concentrated at DOD on the adjudication portion and we have found issues with the adjudication when we did our work back in 2006 and 2008. We found similar issues with the adjudication files as we did with OPM's investigative files" (*The Insider Threat*, 2013, p. 44).
Amount of classified information	"Two problems. One, there is way too much stuff that is classified that does not need to be classified. And, two, there are way too many security clearances approved. So if you markedly increase the amount of material that does not need to be classified, you have to increase the number of people that need to have access to it" (*The Navy Yard Tragedy,* 2013, p. 4).

Each example represents the way the texts were subcategorized to further narrow down the larger category and response to the research questions. For the subcategory adjudications, the textual examples show that Congress is discussing adjudications issues for BIs. As discussed in chapter two, adjudications is the step of the process where an adjudicator decides whether a clearance candidate will be granted or denied a clearance. Although Ms. Farrell, a director at the Government Accountability Office states that they identified adjudicative issues back to 2006, this statement and the hearing from which it was taken questions the ability to correctly issue clearances in a post-Snowden environment. Similarly, the second statement also questions the amount of classified information that exists and the impact of the amount of people who need clearances in order to view that information. The hearing from which this passage was taken explored the connection between Snowden's clearance and his ability to access classified

information. If less information is classified, then fewer people will need clearances. This will further mean fewer will have access to potentially detrimental information.

For the second question addressing how applying another terministic screen changes the interpretation of the congressional communication, I selected eight representative themes of surveillance studies and coded each passage of the documents to see first if the BI fit the characterization of surveillance, and second for a lens to discuss the implications of the first question's findings. As discussed in chapter two, these terms were constancy, surveillant assemblage, surveillers, social sorting, risk, prediction, identity, and technology. Whenever the text represented one of these themes, I coded the text as such. Tables 8-15 illustrate examples of the eight categories. Sample textual passages of the categories are included in Appendix A, B, and D-I. Overall, Table 3 provides the full chart detailing all final categories for question one, and Table 6 details all final categories for research question 2. Table 8 illustrates an entry in the "Constancy" category.

Table 8.

Deductive Results Example – Surveillance: Constancy

Category: Constancy
Definitions: Control comes in the forms of continuous assessment (Deleuze, 1995, p. 182) and "constant monitoring checks worker activities and individual inducements provide incentives for compliance" (Lyon, 2007, p. 60).
Coding Rules: Indication of continuous assessment and continuous assessment with a tangible benefit
Textual Example: "One critical element for a robust security clearance process is to establish an effective capability to assess an individual's continuing eligibility on a more frequent basis" (*The Insider Threat*, 2013, p. 16).

In conversation with surveillance study's employment of the idea of constancy, this passage shows that Congress wants to implement more checks for more frequent assessment. In the context of the hearing from which this passage was taken, Congress is advocating for a continuous evaluation system which constantly monitors those with clearances. It is the hope of

Congress that those with clearances will be subject to constant checks and will "incorporate and analyze data in near real-time" from a number of sources (*The Insider Threat*, 2013, p. 12).

In conjunction with the idea of surveillant assemblage, the passage in Table 9 provides evidence of seemingly unrelated data coalescing for the purpose of government scrutiny. Congress details that data included in the BIs come from multiple places like a subject interview, personal sources, and records. The data is further assembled in a report of investigation, and this information is monitored and assessed to make sure it properly follows the agency's preconceived criteria for risk[36] prevention.

Table 9.

Deductive Results Example – Surveillance: Surveillant Assemblage

Category: Surveillant assemblage
Definitions: Seemingly unrelated data flowing from multiple sources that are "reassembled and scrutinized in the hope of developing strategies of governance, commerce and control" (Haggerty & Ericson, 2000, 613); surveillant assemblages expand surveillance from the idea of one watcher to a larger network and flow of information coming from multiple places (Haggerty & Ericson, 2000); it is more of a distributed collection of information which uses "techniques derived from military, administrative, employment, policing and marketing practices" (Lyon, 2007, p. 95).
Coding Rules: Evidence of data coming from multiple sources
Textual Example: "Field investigations include work such as conducting Enhanced Subject Interviews (ESI), obtaining personal testimony from a variety of source types, conducting record searches, and reporting all information obtained. Specific work requirements include case control/assignment, performance to investigative scope and coverage, reports of investigation, management of inventory, and quality control of deliverables to ensure quality standards are met" (*The Navy Yard Tragedy,* 2013, pp. 121-2).

On the surface, BIs may seem to be a government concern. Congress even thinks so when it questions the use of contractors for "inherently governmental work because it involves secure matters" (*DC Navy Yard Shooting*, 2014, p. 76). While OPM agrees that the ability to adjudicate to grant or deny a clearance should be "made by only government officials" (*Safeguarding Our Nation's Secrets: Examining the Security Clearance Process*, 2013, p. 68), the above statement in Table 10 illustrates that OPM has allowed non-governmental agencies to carry out BI functions.

[36] See the risk and prediction categories in Table 6 for correlating information.

Together with the previous textual example illustrating surveillant assemblage, the texts show that when conducting BIs for security clearances, non-governmental agencies are able to use non-governmental agency information (such as credit reports) in order to carry out governmental objectives. This challenges government-only assumptions of surveillance.

Table 10.

Deductive Results Example – Surveillance: Surveillers

Category: Surveillers
Definitions: "Old lines [of control] become blurred – lines that once distinguished police work from private security, or law enforcement from consumer management" (Lyon, 2007, p. 107).
Coding Rules: Indication of multiple actors gathering surveillance
Textual Example: "The great majority of background investigations (over 90 percent) are performed by the Federal Investigative Services (FIS) within the Office of Personnel Management (OPM), at the request of other agencies, though several agencies, many of which are in the Intelligence Community, are authorized to conduct their own…OPM hires contractors to conduct much of the information collection, and other agencies also use a mix of contractors and federal employees to gather the information needed for a background investigation" (S. 113-276, 2014).

The textual example in Table 11 focuses on databases in order to classify people for differential treatment. As shown, the names of those who have been granted a clearance are inputted into a database which OPM maintains. Because the agency an individual works for (e.g., the Department of Energy) is the agency which determines through adjudications whether an individual should receive a clearance, this passage also highlights the interagency sharing of information through technological means and the role technology plays in allowing special treatment. The Department of Energy would have communicated with OPM in some way to indicate whether a subject of investigation was granted a clearance.

Table 11.

Deductive Results Example – Surveillance: Social Sorting

Category: Social sorting
Definitions: Relies on searchable databases “to determine who should be target for special treatment, suspicion, eligibility, inclusion, access” (Lyon, 2003b, p. 20); "Social sorting refers to a variety of surveillance practices that create various databases and have access to others--public services, police, intelligence, business, consumers - in order to categorize people for different treatment" (Gordon, 2011, p. 167).
Coding Rules: Evidence that information from databases is used for determining outcomes
Textual Example: “OPM maintains a database of federal employees and contractors adjudicated as eligible for clearances. Individuals approved to hold secret security clearances must undergo a reinvestigation every 10 years, and those approved for top-secret clearances must undergo a reinvestigation every 5 years” (USGAO, 2013, p. 2).

The example text in Table 12 provides evidence of what was considered a risk by Congress. As identified by this passage, the form gathers specific information about the applicant to determine if their history exhibits any behavior that, when compared with adjudications criteria, would indicate the individual poses too much risk.

Table 12.

Deductive Results Example – Surveillance: Risk

Category: Risk
Definitions: “Risk refers to external danger, such as a natural disaster, technological catastrophe, or threatening behavior by human beings” (Ericson & Haggerty, 1997, p. 3); in a risk society, “risk communication formats are the focal point for an institutions selection and definition of risks” (Ericson & Haggerty, 1997, p. 9); to know what a risk is, is to know the institutional discourse around the risk - how it is classified, what it means, and how it should be responded to (Ericson & Haggerty, 1997); Surveillance provides the data for risk assessments (Barnard-Wills, 2012, p. 178) and risk types (Staples, 2000)
Coding Rules: Discussions of different types of risks - what are identified by the documents as being risks? Discussions of how to determine risk (i.e., investigative and adjudicative criteria); Discussion of where the background information comes from. What is required for e.g., the SF-86?
Textual Example: “A security investigation begins when the individual, at the request of the sponsoring agency, submits an application in which the individual provides detailed information on a broad range of topics, including: personal history, identity of relatives and friends, foreign

contacts and activities, criminal and legal record, any financial or tax difficulties, use of drugs and alcohol, and other matters" (S. 113-283, 2014).

Identifying risks also works with the idea of prediction and probabilities. Identified risks, if eliminated, may also eliminate possible problematic behavior. As shown in Table 13's sample passage, Congress' discourse suggests that the BI must identify problematic activities in order to eliminate potential future adverse behavior. If say, a BI identifies a subject of investigation has a financial issue, then supposedly this makes the candidate risky and extra scrutiny should be given because the individual's character may be in question. Not granting a person with excessive debts and would possibly keep a future security infraction from happening.[37]

Table 13.

Deductive Results Example – Surveillance: Prediction

Category: Prediction
Definitions: Risk communication systems focus on "calculating probabilities" (Lyon, 2007, p. 38); risk is based on probabilities (Barnard-Wills, 2012, p. 178)
Coding Rules: Indication of attempting to identify problems before they occur; indications of risk probabilities.
Textual Example: "The OPM Background Investigation process must be capable of flagging high-risk individuals holding clearances and alert case officers of situations requiring review before any adverse consequence takes place" (Enhanced, 2013).

As shown in Table 14, this passage shows how identities are defined and how the texts match the definition. The "whole person" concept has been discussed throughout this dissertation, and this passage adds to the conversation by showing that investigations are seeking out derogatory information such as challenges a subject of investigation has faced and subsequent issues that may have emerged. If an adjudicator would be looking at this information, they would be making a determination of the kind of person an individual was based on these

[37] According to Henderson (2010a), "Excessive indebtedness increases the temptation to commit unethical or illegal acts in order to obtain funds to pay off the debts. Most Americans who betrayed their country did it for financial gain..."

pre-existing criteria, to include credit and alcohol use. Supposedly, these things are important in determining if one is trustable with national security information.

Table 14.

Deductive Results Example – Surveillance: Identity

Category: Identity
Definitions: Identities are relational, always involve others, and always change (Lyon, 2009, p. 12); identities are articulated in particular contexts" (Barnard-Wills, 2012, p. 36); in a subjectivist understanding, "identities are not fundamentally given by rather socially constructed" (Barnard-Wills, 2014, p.176)
Coding Rules: Indications that an identity is a comparison to other others; idea that identities can change; resistance to identity
Textual Example: "Well, as part of the reinvestigation process, the previous investigation is looked at for any derogatory information there, looking for trends, looking for ongoing concerns; and it is all part of a whole person concept where you look at what has happened in the person's life, what challenges they have faced, whether or not they have had issues with credit or alcohol, and that is part of the adjudicative process" (*DC Navy Yard Shooting*, 2014, p. 58).

I coded the passage in Table 15 as technology under the subheading of everyday technology because Congress recommends using information such as financial credit history, currency transactions and social media as places for surveillance data. Credit reports and currency transactions are part of personal spending habits, and social media sites are platforms where individuals interact and communicate with their friends or acquaintances. These elements then are essentially monitoring and picking up day-to-day habits of subjects trying to get BIs.

Table 15.

Deductive Results Example – Surveillance: Technology

Category: Technology
Definitions: Power circulates digitally and surveillance is embedded in our daily actions through things such as technology (Deleuze, 1995, p. 178; Lyon, 2007, p. 60)
Coding Rules: Everyday use of tech can be incorporated into BIs
Textual Example: "The plan submitted under subsection (a) shall--…(A) on a continual basis, access Federal, State, and local government and commercially available information, including financial credit history, currency transactions, court records, traffic violations, arrest records, terrorist and criminal watch lists, foreign travel, and online social media…" (H.R. 490, 2015).

Step Six – Draw Conclusions and Detail the Processes

Once the coding has been completed and all material has been accounted for, researchers can further decide how to write up and further document their work. Depending on the overall goal of the study, the researcher can go about this in different ways. According to Schreier (2014), “With qualitative content analysis, the coding frame itself can be the main result…[or] [t]he findings can also serve as a starting point for further data exploration, examining the results of qualitative content analysis for patterns and cooccurrences of selected categories” (p. 180). It can involve just looking at what the results are to drawing larger conclusions such as looking at the relations between the categories or between other texts.

The way the study is written will not only illuminate the study for the researcher, it will also provide validity to the study itself. Elo and Kyngas (2007) describe this in their third phase, or what they call the reporting phase. Results of the study must be written in appropriate ways which can relate the steps the research has gone through. In order to make the study and process as clear as possible, “The analysis process and the results should be described in sufficient detail so that readers have a clear understanding of how the analysis was carried out and its strengths and limitations” (Elo & Kyngas, 2007, p. 112). The results then are an important product of the research, and they should be reached only by a systematic, methodological process that has evolved through multiple readings and category expansions and reductions.

In my study, this dissertation chapter accomplishes the goals of laying out the methods I took in order to conduct my research. In order to ensure credibility and trust with readers by showing the underlying motivations and choices that I made during the research process, I wrote this chapter. It details which steps I took and how I came to my conclusion. Further, chapter four describes the results of the investigation in greater detail, and chapter five provides a discussion on the implications of the study’s results. All chapters of this dissertation, taken together, ground the study in academic literature and accomplish the final product of a methodological and thorough qualitative study.

Criticism and Limitations

Although as shown, qualitative content analysis has systematic processes, criticisms do exist. Because of the qualitative roots of the process, and in addition to the flexibility and the mutability of the research in qualitative content analysis (in which, as discussed, the categories are developed during the scaffolding process and are dependent on the study), some researchers have highlighted the criticisms of qualitative content analysis which suggest qualitative analysis is questionable because it relies on researcher interpretations (Bos & Tarnai, 1999; Elo & Kyngas, 2007; Graneheim & Lundman, 2004). Denzin and Lincoln (2005) point out that some consider the use of quantitative methods a “hard” scientific method built on processes and meanings measured by experiment for “quantity, amount, intensity, or frequency” (p. 10), and qualitative methods as soft science that is unscientific, exploratory, or subjective. As Denzin and Lincoln (2005) continue, some scholars allege that the qualitative research process tends to focus more on the socially constructed nature of information and allege that researchers use interpretation to make sense of data rather than letting the data speak for itself in a supposedly value-free realm of interpretation like some researchers consider quantitative research. Qualitative content analysis, by default then, is subject to these criticisms.

This flexibility of category design and ability to use interpretation also leads to the claim that there is no “correct” way to conduct the research (Bos & Tarnai, 1999; Elo & Kyngas, 2007; Graneheim & Lundman, 2004). This ambiguity in turn causes claims that there isn’t a comprehensive enough handbook or literature on the method to work through the process or address problem areas (Bos & Tarnai, 1999; Elo & Kyngas, 2007). This flexibility and lack of direction then causes researchers to have to judge what is appropriate for the study, and this in turn makes analysis difficult and open to criticism (Elo & Kyngas, 2007). Researchers are thus forced to make interpretations due to this flexibility on what methodological process application is best and what the results mean. Overall then, the amount of interpretation threatens the research, and thus, the method is so flexible that the results should only be seen as a tool rather than actual study (Graneheim & Lundman, 2004).

There are rebuttals to this criticism though. First, although Bos and Tarnai (1999), Elo and Kyngas (2007), and Graneheim & Lundman (2004) reported that some scholars attack the value of qualitative analysis in comparison to quantitative methods, qualitative, like quantitative research, still must adhere to standardized processes of research (Schreier, 2014). Fundamentally, according to Graneheim and Lundman (2004), qualitative content analysis must be valid, reliable, dependable, generalizable, transferable and credible.[38] As seen by the prior discussion of how to conduct a qualitative content analysis, there is a set of steps a researcher must go through in order to do their analysis. Researchers must maintain a sense of uniformity despite the inherent flexibility to the process. The material has to be examined according to relevancy to the research questions, must be examined through a series of steps, and needs to be revised so that the process is representative of the data overall. So, while the method may change for different studies, "the steps and their sequence remain the same" (Schreier, 2014, p. 171). Additionally, counter to the idea that there is not enough research on qualitative content analysis, Bos and Tarnai (1999) show that "there are a series of individual contributions more or less scattered through numerous journals (especially in the last few years) in which the content analysis method is applied or detailed problems inherent in this analytic technique are discussed" (p. 659).

Additionally, just because content analysis may be flexible and at some points open to researcher interpretation, this is not necessarily a weakness that makes information unreliable or not credible. It is not a hidden secret that qualitative analysis uses interpretation. Research on qualitative content analysis openly acknowledges that even though the method may be standardized, there may also be different interpretations based on methodological choices and assumptions (Denzin & Lincoln, 2005; Elo & Kyngas, 2007; Graneheim & Lundman, 2004; Schreier, 2014). Graneheim and Lundman (2004) even conclude, "[I]t is impossible and undesirable for the researcher not to add a particular perspective to the phenomena under study"

[38] According to Graneheim and Lundman (2004), "[C]redibility deals with the focus of the research and refers to confidence in how well data and processes of analysis address the intended focus" (p. 110).

(p. 111). The researchers bring out that this is true of not just qualitative studies but texts in general. They say, “[A] text always involves multiple meanings and there is always some degree of interpretation when approaching a text” (p. 106).

For instance, in my study, because my research questions and eight lenses drove how I was coding my material, I was limited in the way I coded my information. Additionally, the coding that I used informed my interpretations. For instance, looking at adjudications through a lens of social sorting will provide a different analysis compared to looking at adjudications through a lens of risk. The social sorting lens (depending on the specific definition used) will be more aligned with placing subjects of investigation into categories, while an adjudications conversation through a risk lens (again, depending on the specific definition used) would concern the criteria used by adjudications to specify risk.

What is important in this acknowledgement though, is that the methodology, findings and analysis be as transparent as possible to openly account for any of these interpretations. As long as the researcher is open and transparent about their assumptions, the concern about interpretation is diminished. Graneheim and Lundman (2004) add:

> There is no single correct meaning or universal application of research findings, but only the most probable meaning from a particular perspective. In qualitative research, trustworthiness of interpretations deals with establishing arguments for the most probable interpretations. Trustworthiness will increase if the findings are presented in a way that allows the reader to look for alternative interpretations. (p. 110)

One way to help facilitate and demonstrate trust is to provide enough examples which illustrate the way the research was carried out. In order to do this, researchers should present their material comprehensively and provide citations and textual examples which demonstrate the applications of the matrix codes (Graneheim & Lundman, 2004; Hsieh & Shannon, 2005). This chapter of my dissertation especially preforms this task of comprehensively presenting the study’s methods.

Before continuing, it is also of note that despite the criticisms of qualitative analysis, quantitative analysis is also not a without criticism. Despite claims of objectivity, quantitative methods don’t operate without interpretations. As Bos and Tarnai (1999) stated, “According to the basic conception of the Frankfurt School, findings from quantitative investigations must

necessarily be qualitative; otherwise the results remain a dull presentation of figures" (p. 665). In this sense then, it is important to think critically about quantitative research too. It is not just qualitative research that makes interpretations; quantitative researchers have to use judgment too when deciding what to do with their research results.

So overall then, while there may be criticisms to the process, there are also rebuttals for these criticisms. While content analysis may be a more interpretive process where researchers have more freedom and flexibility than other methods and processes to scaffold their study based on their research questions and texts, this does not mean that content analysis and the studies using it aren't systematic and uniform. Using a systematic process to interpret the context of the selected texts is the purpose of qualitative content analysis (Hsieh & Shannon, 2005), and qualitative content analysis is a justifiable and helpful methodology to use "provide knowledge and understanding of the phenomenon under study" (p. 1278).

Conclusion

Overall, qualitative content analysis is a useful methodology which allows BI reform to be explored. By enabling both inductive and deductive structuring, the research questions can be addressed through various ways which allow multiple interpretations of the texts. Although there are criticisms of the process such as the process is too flexible and open to too much interpretation, as discussed the process has fundamental procedures like that should be followed:

1. The researcher decides what needs to be analyzed and selects documents.
2. The researcher becomes familiar with the texts.
3. The researcher constructs a scaffold though which to sort and code the material.
4. Before finalizing the scaffolding, the researcher conducts a pilot study.
5. The researcher then conducts the study and codes the material using the scaffolding.
6. The researcher then draws conclusions and details the processes he/she used to conduct the study.

To combat claims of being too soft of a method that is too dependent on interpretation, the researcher maintains proper documentation of the research process and reports this along with

the results of the study. This study adheres to the methodological guidelines, and conclusions were drawn based off these principles.

CHAPTER 4

RESULTS

To review, I addressed two research questions. My first was 1) based on congressional hearings, bills, daily editions and reports, since Congress began to react to Snowden's disclosures in June 2013, what arguments have emerged in the documents as flaws to the BI process? My secondary question was 2) how does applying another terministic screen change the interpretation of the Congressional communication? This chapter (chapter four) addresses the results of each question for my study. In this chapter, I will first outline what Congress thinks are flaws to the BI process, and I will then categorize the passages into the eight chosen characteristics of surveillance studies so that I can interpret the results of question one in the context of surveillance studies. Chapter five will further look at the most significant conclusions drawn from the two data sources to analyze the implications of my study. [39]

I essentially did an analysis of the same documents in two different ways, so in this chapter, I separate and examine results for each question. For the first question, I briefly discuss each category of result (Overall Process; Oversight; Requirements Determination; Application; Investigation; Adjudication; Appeals; and Periodic Reinvestigation). This category used inductive methods because the categories grew from the passages themselves. For the second question, I discuss each surveillance category (constancy, surveillant assemblage, surveillers, sorting, risk, prediction, identity, and technology) and identify how the passages fit this category. This used deductive methods because I started with the categories and then decided how the passages fit these categories. I then arranged those results inductively in order to further classify them for discussion. [40] After I relate the data from each from each question, I include a small summary of

[39] While there many significant points to expand upon, I define "most significant conclusions" to mean the categories with the most and least attention. In this case, the *application* received the least amount of attention, and *risk* received the most attention in my data collection. I focused on the most and least attention in chapter five due to the project's scope and study's time and space constraints. Future research could look into the many other emergent data points.

[40] The deductive analysis of the data in conjunction with surveillance literature did contain some inductive methods, but the inductive analysis was secondary to the deductive categories. I used the inductive methods in the deductive analysis to be able to sort through the initial deductive results.

the sections. At the end of each question, I also summarize the results of the question. Further, chapter five looks at all these summaries together to identify what I think is the largest implication from the study.

As a point of clarification, the same category may appear in the results of both questions, but if it does, the two categories are not the same and the context of the posts makes the results different. For instance, there are two categories titled technology and utilize passages about technology as a subject of study. The subcategory of technology appearing in the inductive category identified flaws in the BI process but is different than the interpretation of the same passages found in the technology section in the deductive methods analyzed using surveillance studies. The first mostly sees technology as a neutral way to fix BIs, and the second sees technology in a more skeptical view that is a product of human construction. The results differ depending on the terministic screen applied to the passages.

Results of Inductive Study

Inductive methods help answer the first question which addresses the supposed flaws of the BI process. As described in chapter three, inductive methodology applied to qualitative content analysis allows for open coding of information and helps scaffold patterns that begin to emerge from the texts. In the case of this study, there were initially thirty-eight emergent themes that showed up in the reports. To reiterate these results as shown in chapter 3, they are listed in Table 16.

Table 16.

Results of Inductive Methods – Flaws to the BI Process.

Federal BI Flaws – Alphabetical Order		
1. Adjudication 2. Amount of classified info 3. Audits 4. Communication (lack) 5. Contractors 6. Facilities 7. Finances 8. Forms	13. Incomplete investigations 14. Internet/social media 15. Law enforcement 16. Legislation - current 17. Mental health 18. Metrics	25. Quality 26. Reciprocity 27. Reports - Need more 28. Revocation/suspension/appeals 29. Safeguard for employees 30. Self-reporting 31. Speed, efficiency, timeliness 32. Standardization 33. Tax debts/debts 34. Technology

9. Fraud 10. General questions 11. Historical precedence-events 12. Historical precedence-studies	19. More/continuous evaluation 20. National security state 21. Oversight/review 22. Prediction 23. Position designation/# of clearances 24. Process	35. Time between investigations 36. Training 37. Transparency 38. USIS

To discuss these results in manageable chunks, I organized the thirty-eight categories into eight representative categories that I found mostly coincided with the BI process: 1) Overall Process; 2) Oversight; 3) Requirements Determination; 4) Application; 5) Investigation; 6) Adjudication; 7) Appeals; and 8) Periodic Reinvestigation. Six of these are investigation processes (requirements determination; application; investigation; adjudication; appeals; and periodic reinvestigation) first identified by a chart shown in chapter two and shown again in Figure 8. The other two categories, “Overall Process” and “Oversight” I added because the first covers attitudes associated with how the entire investigation is carried out, and the second discusses how to surveil the surveillance. Both categories contained passages that summarized the whole BI process rather than corresponding to specific steps.

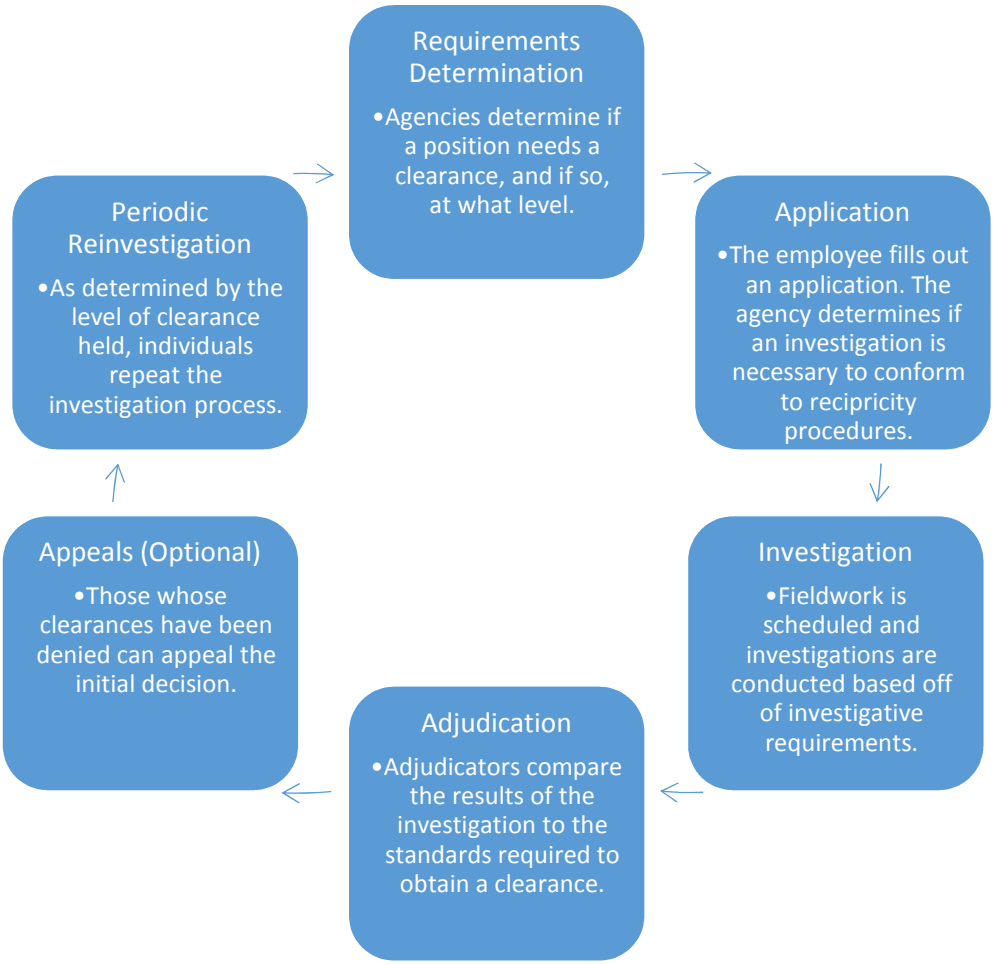

Figure 8. Steps of the BI. Note: Data from *The Navy Yard Tragedy* (2013)

While these categories are not absolute, they do provide a way of seeing and discussing the data in a manageable way.

Table 17 (originally shown in Table 3) offers a broad outline of each category. Figure 9 offers a graphic representation of the amount of passages contained in each category so that it is evident which categories contained the most passages. A further subcategorized chart for each category appears at the beginning of each section, and an outline and chart with sample data appears in the appendix. As discernable from Figure 9, the “Overall Process” category contained the most passages while the “Application” section contained the least.

Table 17.

Overall Results of Inductive Methods.

Federal Flaws - Groups			
Overall Process: • Communication (lack) • Finances • General questions • Historical precedence-studies • Historical precedence - events • Legislation - current • Prediction • Process • Self-reporting • Speed, efficiency, timeliness • Standardization • Technology	**Oversight** • Audits • Metrics • Oversight/ review • Quality • Reports – Need more • Training • Transparency	**Requirements Determination** • Amount of classified info • Position designation/# of clearances • Facilities • National security state	**Application** • Forms • Reciprocity
Investigation • Contractors • Fraud • Incomplete investigations • Internet/social media • Law enforcement • Mental health • Tax debts/debts • USIS	**Adjudication** • Adjudication	**Appeals** • Revocation/ suspension/ appeals • Safeguard for employees	**Periodic Reinvestigation** • More/ continuous evaluation • Time between investigations

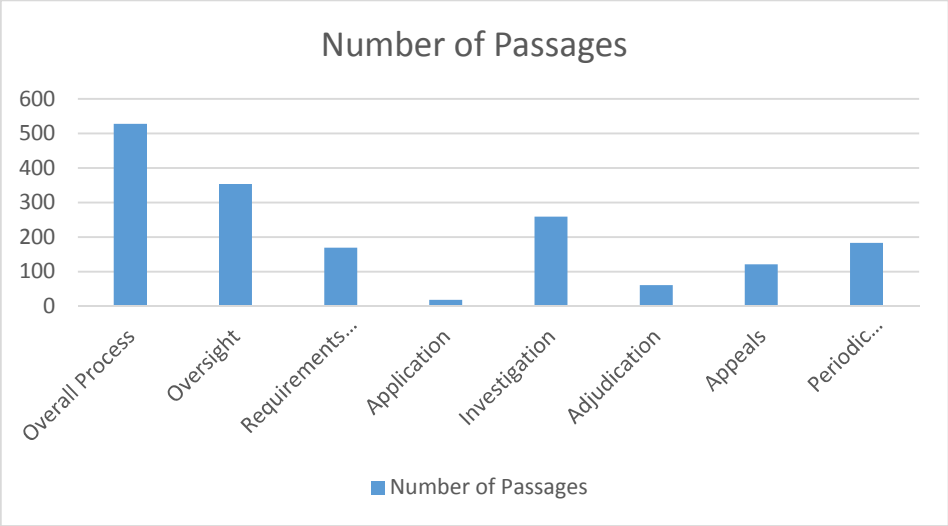

Figure 9. Graphic Representation of Inductive Methods

Overall Process

I'll start out breaking down the results of question one by discussing the "Overall Process" section as it provides a general overview of the entire process and provides a general account of the flaws Congress identifies. Below, listed in Table 18, are the eleven subcategories and further subcategories in this "Overall Process" section. Each reason identified as a flaw in the overall process is listed along with a definition of what that category means and passage example. Each category also lists how many passages are included in each section. An abridged chart for the category is listed in the appendix. Figure 10 provides a graphic breakdown of each subcategory.

Table 18.

Overall Process

Overall Process Total Entries – 528			
Subcategory / Number of Entries	**Further Subcategories**	**Definition**	**Example**
Communication (lack) - 34	• Adjudications • Agencies • Contractor/employees (non-investigators) • Investigators • Law enforcement • Databases	There is not enough communication between BI stakeholders.	"Legislation could also finally allow agency adjudicators to directly speak with OPM investigators, giving adjudicators additional information on an

			applicant when deciding whether or not to grant a clearance" (H. Rep., 2014, p. 3).
Finances - 27	• Inspector General • Designations • Monitoring • OPM • Timeliness	The costs of the investigative process can cause problems.	Although shortening the time for periodic reinvestigations would help identify issues, "it also adds significant cost and resource burdens to federal agencies and to the federal adjudicators" (*The Navy Yard Tragedy*, 2013, p. 100).
General questions - 26	• Questions	Miscellaneous questions posed about the BI.	"But the larger issue is how do we collect—how do we identify and collect relevant information that allows us to constantly adjust our perspective about cleared individuals and individuals who are in trusted positions? And that is really the challenge" (*The Navy Yard Tragedy*, 2013, p. 169).
Historical precedence – events - 140	• 9/11 • Alexis • Elder • Generic recent events • Hasan • Holocaust Museum • Manning • Oklahoma City • Snowden • Wheeling, WV	Events show the BI is flawed, and processes need to change in light of specific events.	"[Snowden]'s investigation "also raises serious questions about what standards are used in reviewing the background investigation and adjudicating a case" (*The Insider Threat*, 2013, p. 2).
Historical precedence-studies - 44	• Continuous evaluation • Legislation-past work • Outdated • Quality • Reports • Timeliness	Studies questioning the BI process have long existed, even before Snowden.	"Since the 1990s, quality in the security clearance investigations has not been a priority" (*The Insider Threat*, 2013, p. 4).
Legislation - 30	• Defense Authorization Bill • General • H.R. 2860 • H.R. 4022 • S. 1276 • S. 1618 • S. 1744 • S. 2061	Legislation is inadequate in scope and needs to be amended.	"According to IRS officials, based on their analysis of the applicable tax laws, IRS cannot disclose tax information of federal employees without taxpayer consent request" (USGAO, 2013, p. 21).

	• S. 2683 • Taxes		
Prediction - 27	• Better processes • High risk • Legislation • Red flags • Predictive metrics • Timely information	There should be more prediction of events.	Adopting this legislation [S. 1618] "represents a sensible path forward to protect national security and to help prevent future tragedies" and is a "common sense solution" (Enhanced, 2013).
Process - 76	• Consequences of bad BIs • Costly • Currently broken • Need new processes • No way to standardize	There was criticism of the whole process and not necessarily faulting one element of the procedure.	"Okay, so they are collecting the data. The problem is it is sort of garbage in, garbage out, and we have flaws in the system" (*DC Navy Yard Shooting*, 2014, p. 51).
Self-reporting - 24	• Examples of self-reporting problems • Need CE and not self-reporting • Vulnerability • What is needed	The self-reporting function of BIs is flawed.	"[B]ecause the system relies on self-reported data, the chances of someone getting caught are minimal. Between 1997 and 2013, of the civilian clearances issued, fewer than one percent were revoked" (Enhanced, 2013).
Speed, efficiency, timeliness - 34	• Cause bad behavior • Examples of why we need • General goal of reform • ME delays • Requesting more information delays • Requirements • Tax delays • Tech	Timeliness is an issue whether it is too fast or too slow.	"There needs to be a balance between processing of clearances quickly enough to allow individuals to do their jobs, but also thoroughly enough to flag potential problems" (Enhanced, 2013)
Technology - 56	• Databases • Need more tech • Problems with tech	Technology is helping, should help more, and remains a source of vulnerability.	One key area for reform should be the increased sharing of information because "there is no government-wide federal database that contains information about individual arrest records by state and local law enforcement entities" (*The Navy Yard Tragedy*, 2013, p. 100).

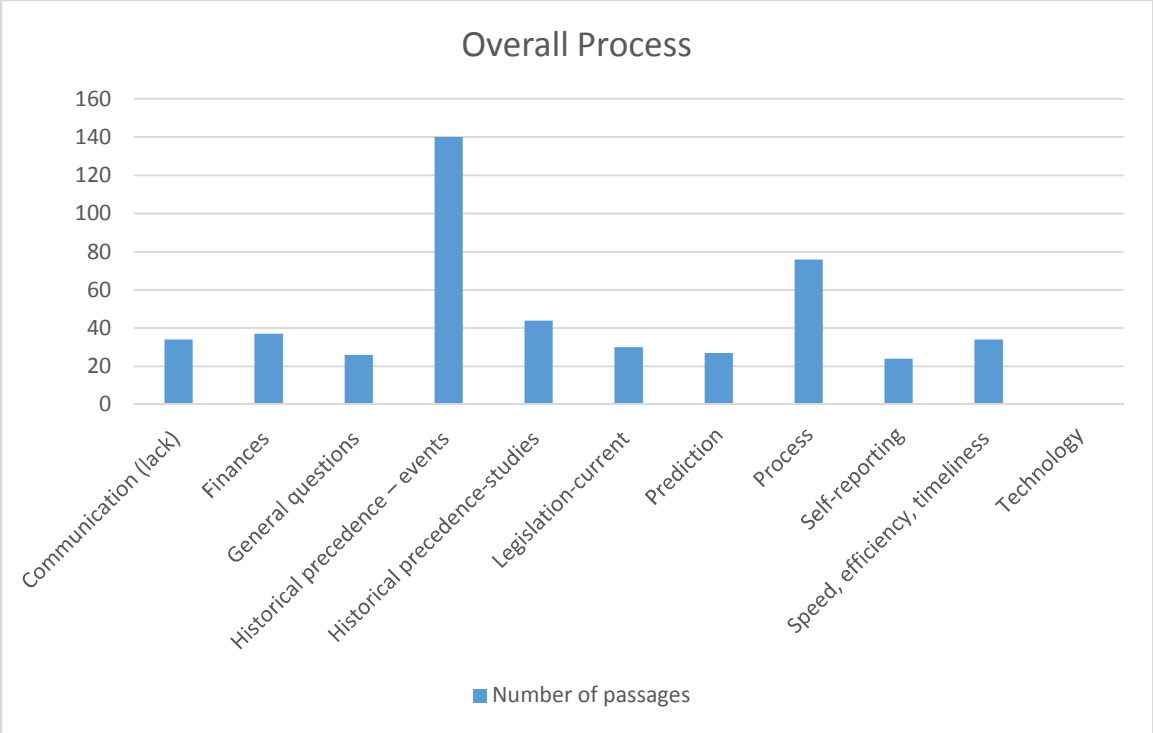

Figure 10. Graphic Results of Overall Process Subcategories

Because this section is so large with no subsection more important than another, I'll provide a brief summary of my interpretations of each subcategory arranged in alphabetical order before I provide my takeaway from this section overall. For each subcategory (in this section and throughout this dissertation), I provide my interpretation of the data based on the number of occurrences. I identify the reoccurring themes and then conclude that due to the emphasis placed on the content of the passages that emerge, the most frequent themes are the most prominent ideas of the section. The passages thus provide the content of which I assign value due to their frequency of occurrence.

The first subcategory in the "Overall Process" category based on the number of passages is "Communication (lack)" and deals with the lack of communication between stakeholders involved in the BI process. This can be between entities such as adjudicators, federal agencies, contractors and employees, investigators, law enforcement agencies, and databases. The second subcategory is "Finances" which deals with the costs involved in the BI program. The major concerns with costs are lack of oversight by OPM's Inspector General (IG), problems with

designations and standards, and delays on timeliness. The third subcategory of "General Questions" is a string of questions posed about the process in general which reveals a concern in how BIs are currently being conducted. The "Historical Precedence – Events" highlights events that have occurred that supposedly prove there is a problem in the process. Examples of cited events used as illustrations of a broken process are 9/11, Alexis, or Snowden. As Figure 10 shows, this section was the largest subcategory in the results. The "Historical Precedence – Studies" is a collection of passages showing that studies have long criticized the BI process even before Snowden and Alexis. The "Legislation – Current" section outlines bills to revise the BI process which have come out since Snowden and Alexis's 2013 actions. "Prediction" concerns the overall belief the BI is flawed because it didn't predict the future. The "Process" subcategory is a collection of passages that insinuate the current process is broken and new processes are needed. As a caveat, there is criticism also as to the ability to standardize processes though, and Gregory Marshall of the Department of Homeland Security (DHS) states regarding facility access and security, "A one-size security solution does not and cannot fit all" (*The Insider Threat*, 2013, p. 12). The "Self-reporting" subcategory talks about the problems resulting from the policy to allow individuals to self-report and adds a call for continuous evaluation. The "Speed, Efficiency, and Timeliness" subcategory talks about how the process takes too long and often causes more problems because investigations are often rushed because they are so time intensive. The passages in the final "Technology" subcategory lead me to conclude that Congress thinks the BI process needs more databases that can be linked across agencies and more technology in general. Interesting though in this category were those that spoke out against technology and saw technology as another potential problem.

Taking all these categories together, my interpretation of this section shows there are many elements considered broken in the BI process overall before even looking as specific steps. From a lack of communication to costs and timeliness, BIs need to be improved and streamlined. Most interesting to these subcategories is that there is still the affirmation that better processes can prevent future attacks. For instance, Representative Darrell Issa states that "best practices in employment could have prevented this [Alexis]" (*DC Navy Yard Shooting*, 2014, p. 2). However,

this section also shows historical precedence that the BI process have had problems before Snowden. For instance, it is not just Snowden causing problems; in the last five years, there have been other security incidents involving cleared employees such as Ricky Elder, Nidal Hasan, Bradley Manning, and Aaron Alexis and problems at facilities such as the Oklahoma City federal building bombings (*The Navy Yard Tragedy*, 2013). Taking history into perspective then, it is not necessarily current costs, self-reporting, speed or lack/presence of technology that have been causing problems since 2013. Problems seem to have existed for periods of time extending before Alexis and Snowden (Young, forthcoming). While the problems with the BI could be related to what is currently being identified as problematic, there could be other issues which are not and have not been addressed.

Despite a history of problems though, Congress is still trying to enact legislation aimed to change the BI process to strengthen the process based on their current identification of issues (113th Cong. Rec. H.R. 2860, 2014; Enhanced Security Clearance Act of 2013, 2013; H.R. 490, 2015; H.R. 4022, 2014; H.R. 5240, 2014; S. 113-111, 2013; S. 113-276, 2014; S. 2683, 2014). However, is interesting to note that the only legislation to have passed by 2015 is the SCORE Act (also S. 1276/H.R. 2860) which give funds to OPM's IG for funds to audit OPM (113th Cong. Rec. H.R. 2860, 2014; S. 113-111, 2013; S. 113-276, 2013). At the time of writing, other legislation such as the CORRECT Act (H.R. 5240, 2014; S. 2683, 2014), SCARE Act (S. 113-276, 2014), the Enhanced Security Clearance Act of 2013 (Enhanced Security Clearance Act of 2013, 2013), the Enhanced Security Clearance Act of 2014 (S. 113-283, 2014), Security Clearance Reform Act of 2014 (H.R. 4022, 2014), and Security Clearance Reform Act of 2015 (H.R. 490, 2015) have all yet to pass.

Oversight

This section deals with specific concerns of the oversight of the BI process. While this element could seemingly fit under the category of the BI process overall, it is also more specifically tailored to surveilling the surveillance. In the documents, the government recommends nine ways that the BI process needs to be examined. Table 19 lists, defines, and

illustrates these recommendations. Figure 11 illustrates the breakdown of each subcategory in graph form. More detailed information is available in the appendix.

Table 19.

Calls for Oversight of the BI Process

Oversight Total Entries – 354			
Subcategory / Number of Entries	**Further Subcategories**	**Definition**	**Example**
Audits - 42	• H.R. 2860 • S. 1276 • S. 2863 • General Concern	More financial oversight is needed for the way OPM spends their money.	"H.R. 2860 would fix the loophole in the current law which prevents this $2 billion revolving fund from paying for the costs of the OPM Inspector General to properly oversee the fund's activities" (113th Cong. Rec. H.R. 2860, 2014).
Contractors - 18	• Contractors	Contractors need to be watched.	"Why weren't we monitoring quality assurance on our contractors to begin with? And what have we done since then to monitor quality assurance on the three contractors that are out there doing it?" (*The Navy Yard Tragedy*, 2013, p. 28).
Metrics - 28	• Overall BI (many concerns) • Quality in particular • Reciprocity in particular • Revocation in particular	There needs to be more and/or uniform assessment for investigations.	"We have seen programs on speeding up the processing of initial clearances, but not on developing metrics for qualitative investigations, implementing those metrics, or reporting on those metrics' findings" (*Safeguarding Our Nation's Secrets: Examining the Security Clearance Process,* 2013, p. 12).
Oversight/review – 81	• Agencies • Continuous evaluation • Facilities • General concerns • OPM • Tech oversight	There needs to be more management (surveillance) of the BI process.	"The fact was, as we knew then [after Snowden], as we know today [after Alexis], we need to make immediate reform of the process. There needs to be more transparency. There needs to be more oversight" (*The Navy Yard Tragedy*, 2013, p. 4).

	• Voluntary is problem for oversight		
Quality - 35	• Agencies • Problems • OPM • Review • Quality control • Stats • Tech • Timeliness	The quality of investigations needs to improve.	"Executive branch agency efforts to improve the personnel security process have emphasized timeliness but not quality" (*Safeguarding Our Nation's Secrets: Examining the Security Clearance Process*, 2013, p. 46).
Reports - Need more - 9	• H.R. 490 • S. 1744 • S. 2863	Agencies should provide more reports to Congress about their clearance efforts and record keeping.	For clearance reform bill H. R. 490, a report should be submitted that "(1) evaluates the quality of background investigations conducted by OPM during the previous year based on the performance measures developed pursuant to the plan submitted under section 2; and (2) includes information on the percentage of background investigations conducted by OPM that meet Federal Investigative Standards (as promulgated by the Director and the Director of National Intelligence)" (H.R. 490, 2015).
Standardization - 112	• Absence of government standards • Followed standards • Go beyond standards? • Legislation • Questions of standards	BI processes need to be standardized.	"OPM has not been doing its job. They were given responsibility by President Eisenhower in Executive Order 10450 and they are supposed to be overseeing how the agencies designate these. I mean, what we have heard today is they are just letting them do whatever, and after this rule, they also will be completely deferential to the heads of these agencies. They have no plans to go back and check whether or not their rule will be applied properly" (USGAO, 2014a, p. 24).
Training - 14	• More training is needed for uniformity	There should be more training on BI processes to get all agencies operating the process according to standards.	National Training Standards will help address BI concerns (*The Navy Yard Tragedy*, 2013, p. 66).

Transparency - 15	• Costs of OPM products • Processes	Being open about BI costs and procedures is important for costs and trust in the process.	There needs to be more transparency in the Revolving Fund program. This will help stewardship of taxpayer dollars. Oversight and openness is something that Archuleta values (Nomination of Hon. Katherine Archuleta, 2013, p. 81).

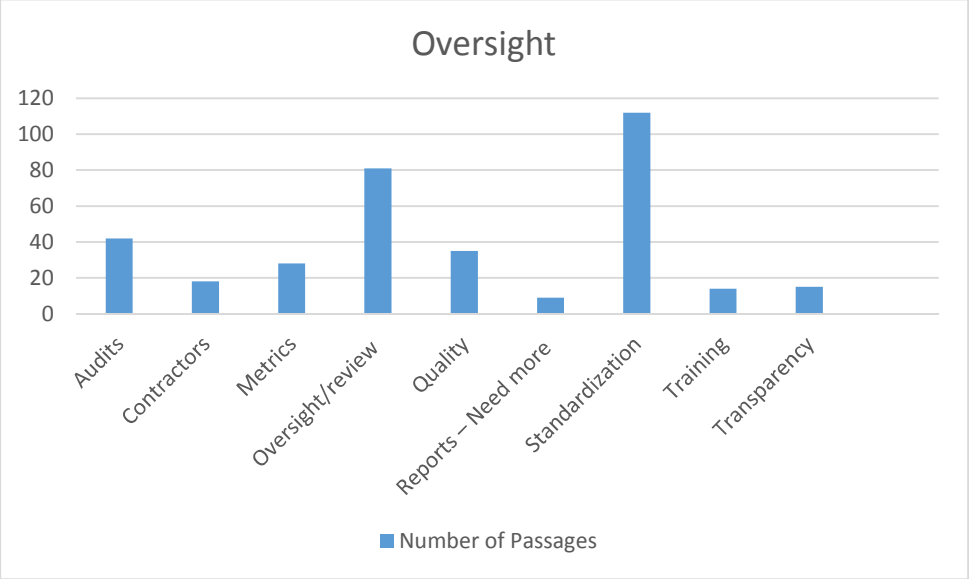

Figure 11. Graphic Results of Oversight Subcategories

Because "Oversight" is also a large category, I will briefly describe each subcategory to get a larger picture of the overall sense of the passages, and then I will address the emerging themes as takeaways. The first subcategory is "Audits," and this section contains passages that call for more audits of the BI process because OPM hasn't had an audit of its funds and procedures. In this section are bills for the SCORE ACT (S. 1276/H.R. 2860)[41] which discusses and calls for more oversight of OPM by OPM's IG. According to the passages, Congress believes that more audits will lead to better investigations (S. 13-111, 2013). Ultimately, the IG declares that OPM's BI program has "been operating in the shadows for too long" and "sunshine is the best disinfectant" (113th Cong. Rec. H.R. 2860, 2014). The "Contractors" section is a general call for the monitoring of contractors so that their actions are scrutinized. The "Metrics" section calls

[41] The SCORE Act became law on 2/2/14 (U.S. Congress, n.d.).

for keeping track of many of the processes associated with the BI to include quality, reciprocity, and revocation of clearances. The passages suggest that this will allow studies of the processes because with uniform policies, aspects of the BI like quality can be measured across agencies (*The Navy Yard Tragedy*, 2013). The "Oversight/review" subcategory is a more general call to provide additional oversight on the process at all steps of BI process. The "Quality" section addresses quality in particular and was included as a separate category due to the number of calls for the monitoring of quality. Quality concerns both the quality of investigative reports (*The Navy Yard Tragedy,* 2013) and quality of the processes of the BI (USGAO, 2014b). The "Reports – More needed" section calls for more reports and is mostly a result of the verbiage from three bills: H.R 490, S. 1744, and S. 2863. These bills all call for reports to Congress on reform measures. As shown in Figure 11, "Standardization" is the largest subcategory in the whole study, and the passages in this section overwhelmingly declare that there is a lack of standardized procedures for the BI especially for position designation, the revocation process, appeals, contractor management, and the self-reporting process. The "Training" subsection discusses that a standardized training program will help make sure all stakeholders are operating on the same page throughout the BI process.

Finally, the "Transparency" subsection is closely related to the audit subsection but puts its own spin on calls for more auditing. This section has passages which call for more auditing and BI pricing so that the process has more openness and oversight (Nomination of Hon. Katherine Archuleta, 2013). Transparency also deals with the correct designation of positions and information so that national security labels aren't overused just to keep information hidden (*Safeguarding Our Nation's Secrets: Examining the National Security Workforce*, 2013). Overwhelmingly, the passages in the "Transparency" category implied that not enough oversight was being conducted, and if more oversight isn't done, then additional bad things beyond Snowden and Alexis will happen. For instance, according to Senator Tester, "The fact was, as we knew then [after Snowden], as we know today [after Alexis], we need to make immediate reform of the process. There needs to be more transparency. There needs to be more oversight" (*The Navy Yard Tragedy*, 2013, p. 4). Also, according to Representative Peter T. King, "[Snowden]'s

investigation “also raises serious questions about what standards are used in reviewing the background investigation and adjudicating a case” (*The Insider Threat to Homeland Security*, 2013, p. 2). Both question the standards underlying the BI process and allude to changes that need to be made in the form of oversight and standardization so that bad events don’t continue to happen, illustrating the concern for a lack of oversight and standards.

In my opinion, the largest takeaway from the “Oversight” section is that the BI process needs to be subjected to more oversight from start to finish in order to make sure the processes work better (*DC Navy Yard Shooting*, 2014) and so that there can be more analysis and studies of the current processes (H.R. 490, 2015). One example calling for more standardization is for position designations, because without standards, clearances are given out “like candy at Halloween” (*Safeguarding Our Nation’s Secrets: Examining the National Security Workforce*, 2013, p. 27), and more clearances causes more risks and costs (USGAO, 2014b). It is also important that the oversight be instituted in large swaths, and the terms *agency-wide*, *department-wide*, *government-wide*, and *across government* collectively occur thirty-five times in the passages for standardization. Judging by this section then, if standards are implemented and oversight is conducted in the forms of audits, metrics, reviews, reports, and training enterprise-wide, then seemingly the BI process will be strengthened. I draw the inference then, that this section calls for more surveillance, of those conducting surveillance.

Requirements Determination

The next section concerns issues related to the phase where an agency determines what information is classified and decides if a clearance is needed to access this information. This is what the government calls requirements determination and is the first official step in the BI process (*The Navy Yard Tragedy*, 2013). Because a clearance is attached to a particular place or person, these designations are decided without regard to a specific individual. Table 20 below outlines and defines this category, subcategories, and further subcategories. Figure 12 provides a graphic illustration of the subcategories.

Table 20.

Reforms Needed in Requirements Determination.

Requirements Determination **Total Entries – 169**			
Subcategories/ Number of Entries	**Further Subcategories**	**Definition**	**Example**
Amount of classified info - 21	• S. 2683 • General Overview • Motives • Number a concern • Snowden	There is too much classified information which requires too many clearances.	"We classify way too much stuff… Because once you create something that is classified, the only people that can work on it are people that have a clearance for that classification or above" (*The Navy Yard Tragedy*, 2013, p. 22).
Position designation/# of clearances - 109	• 9/11 • S. 1744 • S. 2683 • Need standards • Vulnerable/why vulnerable • Why so many	There are a large number of positions designated in need of a clearance resulting in lots of clearances. More clearances results in more costs and more risks.	There are consequences to not properly vetting the workforce. "It is about agencies improperly adjudicating which employees and contractors should be granted a clearance, and it is about pure volume" (*Safeguarding Our Nation's Secrets: Examining the National Security Workforce*, 2013, p. 1).
Facilities - 29	Access	It is important to determine who needs facilities access.	"While nothing can bring back the loved ones who died that day, it is clear that collectively we need to do a better job of securing our military facilities and deciding who gets access to them" (*The Navy Yard Tragedy*, 2013, p. 7).
National security state - 10	Too much classification	Becoming overly protective of information is also detrimental.	"In the wake of the Snowden disclosures, we caution you to guard against over reactions. Excessive secrecy undermines our democracy and threatens our national security by making it harder for us to protect our legitimate secrets" (*Safeguarding Our Nation's*

			Secrets: Examining the National Security Workforce, 2013, pp. 12-13).

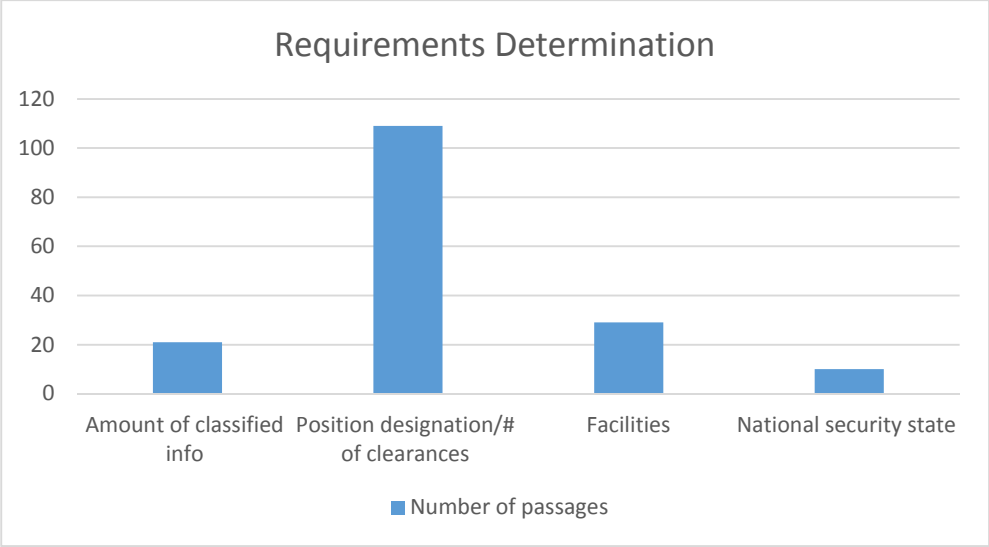

Figure 12. Graphic Results of Requirements Determination Subcategories

Each of the passages in the "Requirements Determination" category address Congress' perceived problems with the BI process at requirements determination step. As a general overview, the first subcategory discusses how information is classified, the second discusses how positions are classified, the third discusses how facilities are classified,[42] and the fourth discusses the idea that there are too many clearances being issued due to too much information being classified thus leading the US to what Angela Canterbury calls a "national security state" (*Safeguarding Our Nation's Secrets: Examining the National Security Workforce*, 2013, p. 12).

Regarding the results of this data, at first I thought that the data would reflect wanting to classify more positions in order to protect information since the whole system of a security clearance is set up to protect specially designated data, but the results were predominately the

[42] An individual needs to have a clearance to access a classified facility like an individual needs a clearance to access classified information. According to chief security officer of the U.S. Department of Homeland Security (DHS) Gregory Marshall, "Using a decision matrix involving mission criticality, the sensitivity of the activities conducted, threats to the facility, facility population of persons who work and visit there, and other factors, an appropriate Federal Security Level is assigned to each facility" (Facility, 2013, p. 19).

opposite. The general idea of this section was that there exists too much classified information causing too many people to have a security clearance and resulting in too many people with access to classified information. This is illustrated by Senator Tom Coburn of the Committee on Homeland Security and Governmental affairs who states, “Two problems. One, there is way too much stuff that is classified that does not need to be classified. And, two, there are way too many security clearances approved. So if you markedly increase the amount of material that does not need to be classified, you have to increase the number of people that need to have access to it” (*The Navy Yard Tragedy*, 2013, p. 4).

One reason for the belief in both too much classified information and too many positions to access this information is the perceived lack of standardization of both matters. For instance, regarding the amount of classified information, Angela Canterbury, Director of Public Policy for the *Project On Government Oversight (POGO),* suggests that agencies have “nearly unbridled power” to determine if something should be considered classified (*Safeguarding Our Nation’s Secrets: Examining the National Security Workforce*, 2013, p. 13), and concerning position designations, Canterbury states, “OPM has failed to appropriately oversee the use of these designations by agencies” and for DOD and DHS this includes the potential to declare “virtually any position as national security sensitive” (p. 68). Jon Tester, chairman of the Subcommittee on Efficiency and Effectiveness of Federal Programs and the Federal Workforce, adds, “Lacking appropriate guidance for such designations, Federal agencies are currently relying on a patchwork of Executive Orders (EO), Federal regulations, and an Office of Personnel Management (OPM) position designation tool that was not created to address security-related issues” (p. 2). Both of these issues are such a concern that Congress took action, and Senate Bill 2683, also called the Clearance and Over-Classification Reform and Reduction (CORRECT) Act, was drafted to streamline both processes by recommending a review of both the number of positions and the amount of classified information in those positions. Part of the verbiage of the Act recommends that the heads of agencies “establish an effective and transparent process” for the designation of security clearances and that there be a push to declassify documents as well as a “ten percent reduction in holdings of classified information” (S. 2683, 2014).

For Congress, the amount of information that is classified and the amount of those needing access to that information causes problems for BIs. First, the larger the amount of sensitive documents and information, the more clearances are needed (*Safeguarding Our Nation's Secrets: Examining the Security Clearance Process*, 2013, p. 2). If more information is deemed classified, more individuals will need clearances, and this need for clearances will produce vulnerabilities and risk of information being divulged. Senator Turner alluded to this when he asked the question, "Are you concerned at all that the amount of classified material post-9/11 may be resulting in a proliferation of individuals having clearance; the fact that the data that we now consider to be classified is so voluminous that, in fact, it is pushing the system in providing increased classified status to individuals?" (*DC Navy Yard Shooting*, 2014, p. 55).

Additionally, more clearances will also cost agencies more money, and more money is bad because agencies don't have unlimited budgets. According to the GAO, "We have previously reported that, to safeguard classified data and manage costs, agencies need an effective process to determine whether positions require a clearance and, if so, at what level" (*Safeguarding Our Nation's Secrets: Examining the Security Clearance Process*, 2013, p. 50).

In addition to the costs of more BIs, there is also a risk that with more clearances, more inaccurate clearance determinations will be made. According to Brenda Farrell at the US Government Accountability Office (USGAO), "Underdesignating positions can lead to security risks while overdesignating can also lead to security risks and result in significant cost implications" (*Safeguarding Our Nation's Secrets: Examining the Security Clearance Process*, 2013, p. 12). While underdesignating may be a problem for security because supposedly less-vetted individuals will have access to more sensitive information, overdesignation is also a problem for costs because, as the GAO continues, "Specifically, the investigative workload for a top secret clearance is about 20 times greater than that of a secret clearance because it must be periodically reinvestigated twice as often as secret clearance investigations (every 5 years versus every 10 years) and requires 10 times as many investigative staff hours" (*Safeguarding Our Nation's Secrets: Examining the National Security Workforce*, 2013, p. 58). If a position is determined to be Top Secret instead of Secret like it should have been, then the costs could rise

exponentially. Specifically, according to the GAO, “The fiscal year 2014 base price for an initial top secret clearance investigation conducted by OPM is $3,959 and the cost of a periodic reinvestigation is $2,768. The base price of an investigation for a secret clearance is $272. If issues are identified during the course of an investigation for a secret clearance, additional costs may be incurred” (p. 58). There is clearly a large difference between a Secret and Top Secret clearance.

Over-designation is not just a concern of costs though, and another issue that emerged in this category was the purposeful designations of clearances in order to obfuscate information. Senator Rob Portman makes the claim, “I think, not making that information available to the public might be one reason the national security sector sometimes is interested in classifying, even when it might not have a national security implication” (*Safeguarding Our Nation’s Secrets: Examining the National Security* Workforce, 2013, p. 17). So much information is being classified and so many positions are being deemed sensitive that some have said the US is moving to a national security state. Canterbury lays out, “The evidence for the growing national security State [sic] is disturbing. As you mentioned, Chairman, we have almost five million security clearance holders. Approximately 20 million four-drawer filing cabinets could be filled with the amount of classified data accumulated every 18 months by just one international agency, according to the GAO” (*Safeguarding Our Nation’s Secrets: Examining the National Security Workforce*, 2013, p. 13). With all this information, agencies can use improper designations to hide what they are doing. Ultimately, Canterbury concludes, “Excessive secrecy undermines our democracy and threatens our national security by making it harder to protect or legitimate secrets. There must be more balance" (*Safeguarding Our Nation’s Secrets: Examining the National Security Workforce*, 2013, p. 74).

Another problem clearance designations leads to is a problem with appealing these designations. The court decision of Kaplan v. Conyers eliminated appearances for certain security designations before the Merit Systems Protection Board. According to Colleen Kelley, National President of the National Treasure Employees Union, this is dangerous because Conyers gives agencies encouragement to have more positions as "sensitive" so that there can

be no review if an employee is fired. An agency could possibly designate a position as sensitive just to get rid of an unpopular employee, and it could be "for reasons motivated by an employee's race, religion, or constitutionally protected speech; it can be for retaliatory reasons; it can be because the employee is a whistleblower" (*Safeguarding Our Nation's Secrets: Examining the National Security Workforce*, 2013, p. 77). And because of Kaplan V. Conyers, an employee may not have the right to challenge their designation. If an employer didn't like someone, the employer could re-designate his/her position as sensitive, and the employee would not have any recourse to fight this designation. The magnitude of over-designations can be seen at CBP where almost all of the 24,000 bargaining unit positions are designated as noncritical-sensitive but only a small number need clearances (*Safeguarding Our Nation's Secrets: Examining the National Security Workforce*, 2013, p. 77).

I find the biggest takeaway from passages associated with requirements determination is that Congress calls for more oversight and standardization of this step because position designations and amount of classified information is problematic. Too much classified information and too many clearances can lead to the wrong people having access to facilities, too many people with access to classified information because too much information is classified (and some not able to appeal adverse actions), and this is leading to a less-transparent society or "national security state." As also discussed in the oversight section, more oversight is needed on these matters, and more standardization should be put in place so that agencies have the same criteria for their people and information.

Application

The application category concerns matters associated with initiating the clearance. In addition to this section covering the actual filling out of the application, according to the GAO

(USGAO, 2013), in this phase, suitability[43] and reciprocity[44] are determined. Suitability verifies whether the applicant is even eligible to apply for a security clearance in the first place, and reciprocity evaluates whether an applicant has already had a background investigation conducted on him/her. If an individual already has a clearance granted by another agency, the second agency can use the first agency's completed BI to grant their clearance without having to conduct field work or having to redo field work due to the rule of reciprocity. Because this dissertation focuses on security clearances, I didn't focus on suitability because this is a separate process and the documents did not address this in depth as a part of the BI for a *security clearance*. I will however discuss reciprocity because this is part of the clearance process since reciprocity concerns accepting another agency's BI for the granting of a clearance.

As shown in Figure 9 and below in Table 21, the "Application" category was the smallest category of the results. Additionally, the fifteen passages of this category mostly centered on the problems with reciprocity. I identified only three passages focused on problems with the application process or involving the form itself. The application section had the fewest passages overall in this category which is interesting considering the BI is based off of the information from the application. Table 21 offers a definition and example of this section, and abridged information is available in the appendix. Figure 13 offers a breakdown of both subcategories.

Table 21.

Reforms Needed in Requirements Determination.

Application **Total Entries – 18**			
Subcategory/ Number of Entries	**Further Subcategories**	**Definition**	**Example**

[43] Suitability is different than a security clearance. According to government finance specialist Henry Hogue, a suitability check "is designed to determine whether a person should be hired for government employment, while a security clearance is used to determine eligibility for access to classified national security information" (Congressional Research Service, 2014, p. 11). For more information on suitability, see https://news.clearancejobs.com/2014/03/15/difference-suitability-security-clearance/

[44] According to Farrell at the GAO, reciprocity is an agency's acceptance of a background investigation or clearance determination completed by any authorized investigative or adjudicative agency" (*The Insider Threat to Homeland Security*, 2013, p. 22).

Forms -3	• Reform the forms	The investigative paperwork needs reform.	The SF-86 needs revision (*The Navy Yard Tragedy*, 2013, p. 67).
Reciprocity - 15	• Matters of reciprocity	Agencies need to share data about acceptance/ honoring of another agency's investigation and granting of a clearance -it may also be a risk not to.	"...even after significant intra-governmental effort, meaningful reciprocity remains elusive" (*The Navy Yard Tragedy*, 2013, p. 99)

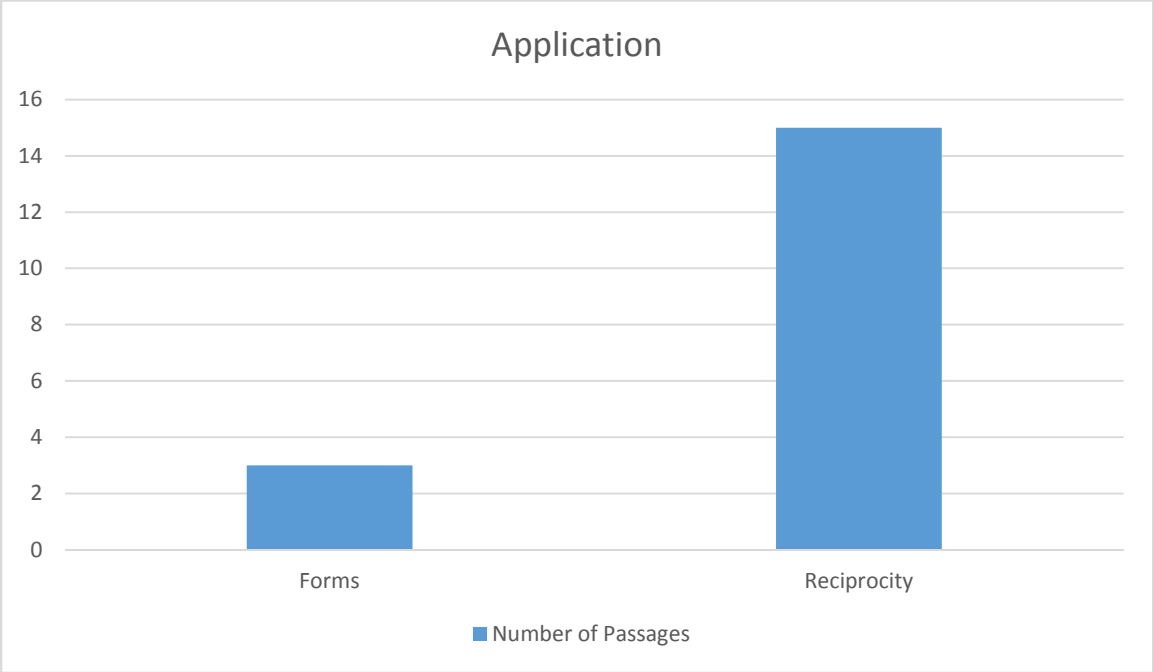

Figure 13. Graphic Results of Application Subcategories

Regarding the subcategory of forms, there were only three passages. Summarizing the results, one passage from Prioletti called for the overall reform of the SF-86 (*The Navy Yard Tragedy*, 2013); one passage from the Professional Services Council (PSC) suggested a new application process calling for "one application, one investigation, one adjudication and one clearance" to standardize all processes BI to ensure reciprocity, and the third was an anecdotal story by Senator Ron Johnson about a former Deputy Secretary of Defense's clearance that seemed overdone and unnecessary. This passage stated, "He [John Hamre] had already filed his electronic version of an SF86. But it was somewhere on a government computer and could not be retrieved. He had to fill it out again, a 4-hour process. His subsequent review was a government employee or a contract employee going through question by question" (*Safeguarding Our*

Nation's Secrets: Examining the Security Clearance Process, 2013, p. 5). The document further recommended more overall standardized procedures which would eliminate these seemingly needless processes.

There are several interesting points from these passages. First, as for recommendations for what an alternative form would look like, in Prioletti's case there was no elaboration on the vision of an updated SF-86. Additionally, the PSC didn't outline what their "Four Ones" process entailed. The third passage from Senator Johnson alluded to a change that would look more like businesses outside the government and continues that Hamre contrasts his SF-86 episode "with his experience in the private sector, answering five questions which had a 99-percent reveal rate in terms of whether that person was committing fraud" (*Safeguarding Our Nation's Secrets: Examining the Security Clearance Process*, 2013, p. 5). Overall in this section though, there was no mention of what an SF-86 version inspired by the private sector would look like.[45] Overall, while all three of these statements called for a change, what that change would look like not addressed.

Second, the motivations of the reforms are also of note. Prioletti said the SF-86 reform should be to "collect accurate information pertinent to today's security and counterintelligence concerns" (p. 67).[46] The PSC alluded to a reform that would help reciprocity (more standardization would make comparisons of BIs between agencies more streamlined), and Johnson suggested that maybe the form should be reduced to be timelier and more effective. Each represents a different reason for recommending the clearance change. Prioletti's position

[45] According to Hamre, "I once served on the board of a major company that collected computer records and provided knowledge services (for example, credit reports) and customer verification services to the insurance industry. The company could detect fraud in more than 99 percent of cases by asking a potential claimant five questions along the lines of: 'Did you live at 123 Maple Ave., 345 Apple Ave. or 456 Oak Ave.?' 'At 123 Maple Ave., did your house have two bathrooms, two and a half, or four?' 'Did the house at 345 Apple Ave. have one fireplace, two or none?' It needed only five such questions. Why, then, does OPM have workers reading applicants the forms that the applicants themselves have filled out, then asking whether this is the truth?" (Hamre, 2013). Again though, an SF-86 inspired by this idea was not discussed by Congress.

[46] Although Prioletti doesn't go into specifics on what the updated information would look like, Stewart (2013) brings out that current investigations are "only looking for very specific behaviors in the subject's past, such as criminal behavior, debt, mental health issues or drug use" which gives insight on how questions could be improved.

aligned more with changing the questions to adapt to a changing society, while the PSC and Johnson's reasons were more procedural to streamline operations.

Regarding the second category of reciprocity, many of the passages suggest that reciprocity is a difficult process to coordinate for several reasons which ultimately causes problems for the BI. First, agencies have a hard time determining what clearances should be granted reciprocity because of the lack of communication between agencies. Prioletti says, "Barriers to reciprocity are the doubt of quality/comprehensiveness of another agency's investigation and application of suitability concerns specific to the receiving agency" (*The Navy Yard Tragedy*, 2013, p. 125). Agencies are thus skeptical of what another agency considers appropriate which may cause an agency to reject reciprocity. For instance, imagine OPM conducts one background investigation. Using this BI, an applicant is hired at Customs and Border Protection. The individual, however, after a year wants to transfer to Immigration and Customs Enforcement. However, because these are two different agencies, each agency doubts the other's decision-making standards for what is an acceptable result of a BI. The second agency may decide to redo the clearance in order to make their own decision. There is merit to this fear as shown by Alexis in the following testimony, though. According to Greg Marshall, Chief Security Officer, US Department of Homeland Security:

> Mr. Alexis had a security clearance with the Navy. When he left the Navy, it was still an in-scope clearance, meaning that the investigation was within the required time frame in order for the organization he was going to to [sic] accept that investigation on reciprocity. We are required by Executive Order in the Federal Government to accept security clearances on reciprocity if there is an investigation that we can point to. The one thing about reciprocity is that we are also required to accept it on its face. We are not allowed to do any additional checks unless we have information—derogatory information to the contrary. So, it looks to me, not having been briefed, that the contracting company accepted Mr. Alexis's security clearance on reciprocity, which was one gap, without having to do additional checks. That also there was a faulty investigation. There was information within the investigation that was done by a private contractor that wasn't accurate. So, it was almost like a perfect storm. It was a gap that was— it was unfortunately hard to overcome. (*Facility Protection*, 2013, p. 46)

This skepticism is ultimately due to the second problem which is a perceived lack of standardization in the reciprocity and BI process. This is discussed in the oversight category, but it also shows up here since reciprocity is a concern for the application process. Although OPM ostensibly has standards of reciprocity for investigations that they conduct (*The Navy Yard*

Tragedy, 2013), according to Senator Tester, the application of the standards varies, which causes Tester to conclude, "consequently there is no reciprocity, and the standards could go from soup to nuts" (*Safeguarding Our Nation's Secrets: Examining the Security Clearance Process*, 2013, p. 23). Further, there is no oversight gauging how many clearances are granted on reciprocity, which makes the process difficult to study and leads the GAO to conclude, "Without comprehensive, standardized metrics to track reciprocity and consistent documentation of the findings, decision makers will not have a complete picture of the extent to which reciprocity is granted or the challenges that agencies face when attempting to honor previously granted security clearances" (*The Navy Yard Tragedy*, 2013, pp. 90-1).

Together, both the form and reciprocity sections show that Congress is interested in reforming the application and application process. There really aren't any specific passages which detail what that reform would look like, but the passages do highlight the need for reform in the form of updated questions, a timelier process, and more standardization for more agency trust. Interestingly, there was not much discussion about the application process, and although investigations are based off the paperwork, there was not much discourse devoted towards reforming this form. This will be discussed further in chapter 5 of this dissertation when the implications of the findings are discussed.

Investigation

This section deals with the problems Congress identifies with the investigation step. According to the US Government Accountability Office (USGAO), the investigation step involves a review of the SF-86 and credit report (USGAO, 2013). For the purpose of this study, I interpreted this step as concerning both the steps of the investigation as well as those doing the investigation and those being investigated. There were ten subcategories in this section detailed in Table 22. The table also provides definitions and examples of the category and further subcategories. Figure 14 offers a breakdown of the further subcategories. Additional sample textual passages are included in Appendix N.

Table 22.

Reforms Needed in Investigation

Investigation Total Entries - 259			
Subcategory / Number of Entries	**Further Subcategories**	**Definition**	**Example**
Contractors - 41	• Contractors causing trouble for government • Different standards? • Government IT systems • Government problem with contractors • Less quality	Contractors and contractor oversight poses problems.	"A contributing reason for these shortfalls is that agencies had not documented procedures for officials to follow in order to effectively oversee contractor performance. Until these agencies develop, document, and implement specific procedures for overseeing contractors, they will have reduced assurance that the contractors are adequately securing and protecting agency information" (USGAO, 2014a, introduction).
Fraud - 38	• Contractor • Employee • Federal legislation • General	Investigators committing fraud and BIs conducted by fraudulent investigators pose risks.	"The term 'covered misconduct' is defined as misconduct affecting the integrity of a background investigation, including falsification or other serious misconduct that compromises the integrity of a background investigation" (S. 113-276, 2014).
Incomplete investigations - 25	• Amount	Investigations are often	"The results are consistent – OPM

	• Using incomplete information	submitted incomplete.	has a problem maintaining the quality of its investigations. A 2009 GAO study, for example, found that 87 percent of OPM investigations were incomplete" (H. Rep., 2014, p. 24).
Internet/social media - 7	• No use of Internet	The Internet can't be used in investigations.	"The current Handbook guidelines strictly prohibit the use of the internet to obtain information about an investigative Subject. The Handbook does not address the use of social media, but instead includes a near-blanket restriction on the use of the Internet" (H. Rep., 2014, p. 36).
Law enforcement - 52	• Can't get information • Consequences • Don't have to get • Fail to get/report information	Law enforcement information is often hard to get or incomplete.	"OPM maintains a list of local law enforcement jurisdictions that do not fully cooperate with security clearance investigators. That list currently includes more than 450 jurisdictions, ranging from small counties to entire states, and including numerous areas with large populations" (H. Rep., 2014, p. 17).
Mental health - 19	• Complex issue • General • In hindsight	Mental health information is needed but often hard to access.	Not addressing mental health issues "poses a vulnerability and risk to the Department"

			(*Facility Protection*, 2013, p. 54).
Tax debts/debts - 29	• Hard to get tax information	Tax debt poses risks, but the data is difficult to obtain.	"Federal agencies generally do not have routine mechanisms to review federal tax compliance for individuals who hold security clearances. Specifically, there is no process to detect unpaid federal tax debts accrued after an individual has been favorably adjudicated as eligible for a security clearance unless it is self-reported, reported by a security manager due to garnishment of wages, or discovered during a clearance reinvestigation (renewal) or upgrade" (USGAO, 2013, p. 20).
USIS - 48	• Conflict of interest • Falsification • Faulty work	The contractor USIS has caused problems for the BI.	"USIS has been accused by one of its own long-time employees of a massive, multi-year contracting fraud scheme" (*DC Navy Yard Shooting*, 2014, p. 132).

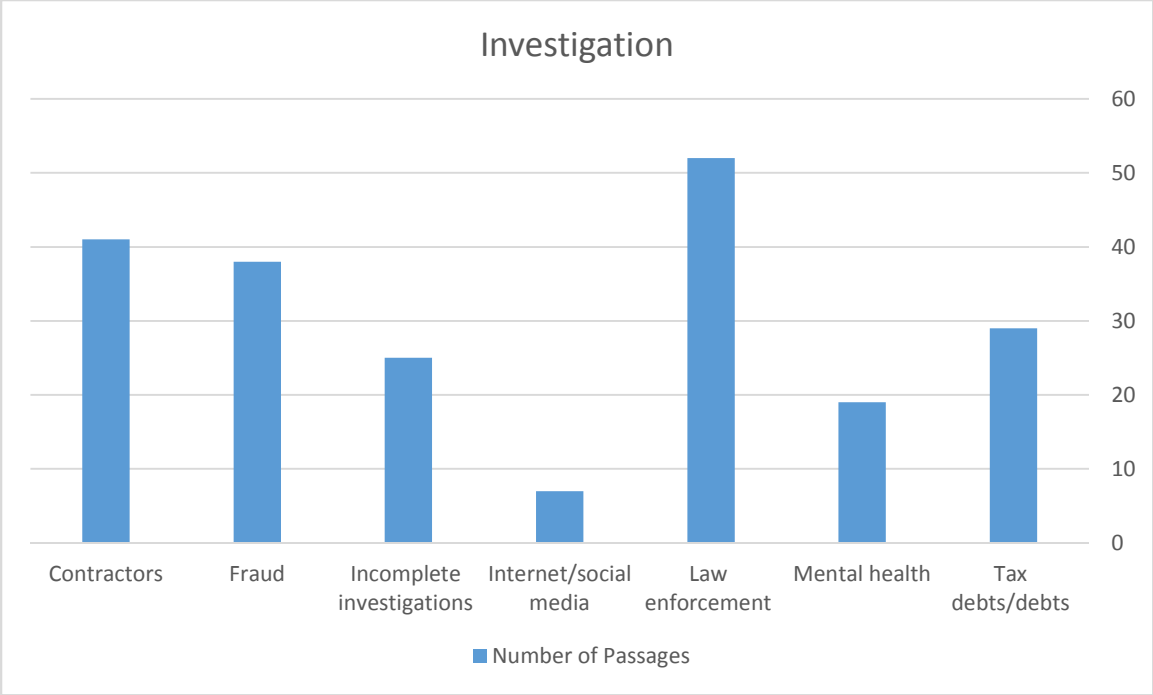

Figure 14. Graphic Results of Investigation Subcategories

As an overall summary, the subcategories of this section described a broken investigative process. The first subcategory of "Contractor" is populated with passages that addressed the general concept of contractors and showed how contractors[47] cause problems for the BI process. For instance, according to Elaine Kaplan at OPM, on average weekly, OPM gets about 55,000-60,000 field work cases completed by contractors, and approx. 3.3% is returned for not meeting standards (*The Navy Yard Tragedy*, 2013, p. 118). Emerging themes were fraud, failures of contract management, and concerns that the quality of BIs is worse for contractors in comparison to employees. Another subcategory is "Fraud," and passages under this heading addressed fraud concerning employees *and* contractors[48] and highlighted legislation proposed to curtail fraud and falsification. For instance, the CORRECT Act recommends that those that falsify be removed from a contract or employment and subjected to prison terms (S. 2683, 2014). The next

[47] As a caveat, USIS is a contractor, but it is under its own subcategory due to the number of passages about it.

[48] Contractor either refers to an individual as a contractor or a company as a contracting agency.

subcategory “Incomplete Investigations” addressed issues discussed in the adjudications section too. Incomplete investigations are frequently submitted, and according to the GAO, a sample of investigations resulted in an 87% deficient rate (H. Rep., 2014). Additionally, there is a lack of standardization regarding if and when agencies should accept and adjudicate these clearances or when they should reject them and send them back to OPM. This matter is discussed more fully in the adjudications section. The “Internet/social media” subcategory discussed how Internet use is not allowed for either investigators or adjudicators. However, continuous evaluation programs are hoping to incorporate social media, so this may change.[49] The next subcategory is “Law Enforcement,” and passages from this section discussed the lack of cooperation between investigators and law enforcement agencies. The next section is “Mental Health,” and passages here showed that it is important to obtain mental health information about subjects of investigation but acknowledge that this is often hard and time-consuming. The “Tax debts/debts” subcategory showed how debts are used to analyze one’s character, but due to regulations, tax information isn’t shared with investigators and the process to get tax information is often hard and time-consuming. The final subcategory is “USIS,” and this builds on the issue of contractors but focused specifically on USIS. These passages showed allegations of fraud and conflict of interest because the company reviewed their own investigations which allowed their falsification scam.

For overall takeaways from this section, there were several interesting points. First, the amount of entries of contractors versus employees significant. While USIS does put the focus on contractors, the general discussion of contractors seemed to insinuate that contractors are questionable compared to employees and may even be inappropriate to use. This is illustrated by verbiage from the CORRECT Act which wanted to reduce the role of contractors and at one point states, “One issue raised by Committee members was the appropriate role of contractors in conducting background investigations” (S. 113-257, 2014). However, the argument is countered by Merton Miller, Associate Director of Investigations for OPM FIS, who shows that contractors

[49] In the late stages of this dissertation’s production, ODNI issued a press release with updated policies allowing for the use of public social media information in BIs effective May 21, 2016 (ODNI, 2016). As this is a new directive, it is not known how this information is carried out, and at this point there appears to be no current change to the Standard Forms.

and employees are trained in the same way, and the only thing that differs is that contractors are paid less and can be fired more easily (*Safeguarding Our Nation's Secrets: Examining the Security Clearance Process*, 2013) which is supposedly better for the government, not worse.

Also, lack of depth in discussion of the use of the Internet is also of significance. There were only a few documents (*DC Navy Yard Shooting, 2014;* Enhanced Security Clearance Act of 2013, 2013; H. Rep., 2014; S. 113-283, 2014) that really spoke about the need to incorporate the Internet into BIs. Considering how big the Internet is in peoples' lives and how Maine Senator Susan Collins brought up Alexis' tragic situation could have been "potentially averted" with knowledge of Alexis' social media trail (Enhanced, 2013), this seems problematic.

There is also an excessive number of tax-related entries which can be explained by one article focusing on this subject. However, the focus on financial information overall is interesting, especially when paired with David A. Borer of the American Federation of Government Employees' comment when he says, "The implication that financial hardship equates to disloyalty, even for employees with no access to classified information, is unsupported and offensive" (*Safeguarding Our Nation's Secrets: Examining the National Security Workforce*, 2013, p. 10). It raises questions on this criteria and other BI criteria which is discussed in more depth in chapter five.

Adjudication

The adjudication section concerns matters of adjudication. As illustrated in Figure 2, adjudication involves the agency who ordered the background investigation through OPM. This sponsoring agency receives the BI conducted by OPM, and then, supposedly based off a set of thirteen standardized adjudication standards, [50] the agency[51] decides whether the individual should or should not receive a clearance (*The Navy Yard Tragedy*, 2013, p. 81).

[50] The category of adjudication in this section address the problems Congress attributed to adjudication and is not focused on the specific criteria of the adjudications process itself. For more information about the adjudicative criteria, see http://www.fas.org/sgp/isoo/guidelines.html.

[51] Neither OPM nor any other agency beyond the sponsoring agency (to include the contractor for whom the subject is working for as in Sowden's case of the contractor Booz Allen Hamilton) decides whether the subject receives a clearance (H. Rep., 2014).

There was only one subcategory in this section: “Adjudication Problems” and five further subcategories in the adjudication problems category: 1) Lack of information; 2) Must be government deciding; 3) Results of bad BIs; 4) Risks; and 5) Standards. Standards are also covered in the “Oversight” section, but they appear here too because they involve problems with adjudication specifically, which is what the research questions were attempting to analyze. Table 23 illustrates this information, and Figure 15 represents the amount of passages in the subcategory.

Table 23.

Reforms Needed in Adjudication.

Adjudication Total entries – 61			
Subcategory / Number of Entries	**Further Subcategories**	**Definition**	**Example**
Adjudications problems - 61	• Lack of information • Must be government deciding • Results of bad BIs • Risks • Standards	Investigative information is often lacking in files for adjudication	“Key information sometimes does not reach the agency adjudicators, which means that individuals—such as Aaron Alexis—are occasionally granted clearances that, had the adjudicator been aware of all the pertinent information, should have received more scrutiny and could have been denied” (H. Rep., 2014, p. 2).

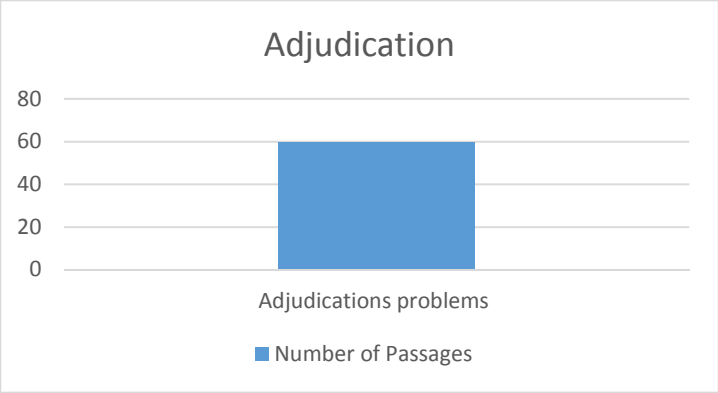

Figure 15. Graphic Results of Adjudication Subcategories

When looking at this section, an overall summary of the results focused predominantly on the problems associated with lack of information in the report of investigation that adjudicators review. This deficiency is well-illustrated by a 2009 analysis that the GAO did of the DOD files. According to their report, "87 percent of investigative reports that DOD adjudicators used to make clearance decisions were missing background documentation" (*Safeguarding Our Nation's Secrets: Examining the Security Clearance Process*, 2013, p. 16), and further in the same report, "22 percent of about 3,500 initial top secret clearances that were adjudicated favorably did not contain all the required documentation" (*The Navy Yard Tragedy*, 2013, p. 73). By 2013 after Alexis' actions, DOD adjudicators stated that 70-80% of OPM's investigative files are still missing information (H. Rep., 2014).

The GAO found that the information typically absent from the reports are "[e]mployment verification and discussions with the employers; social references, especially the number of social references in order to determine someone's character; [and] completeness of the application" (*The Navy Yard Tragedy*, 2013, p. 40). Also frequently missing are sources to verify residences (*DC Navy Yard Shooting,* 2014), interviews with the subjects (*Safeguarding Our Nation's Secrets: Examining the Security Clearance Process*, 2013, p. 17), tax information (USGAO, 2013, p. 27), "documentation of debt repayment or payment arrangements" (H. Rep., 2014, p. 30), and lack of complete records of police reports and criminal record checks (*The Navy Yard Tragedy*, 2013, p. 87).

Counterarguments to the criticism of this missing information are that there are mitigating circumstances that make it difficult to acquire all needed information. It is important to pay attention to the counterarguments because on the surface, it may seem very problematic to have such deficient cases, but real-life factors often get in the way of completing investigations entirely. In some cases, no matter how hard an investigator tried, all information needed in an investigation for adjudications may not be able to be obtained. For instance, some of this missing information is a result of neighbors that have moved away from a subject's former residence (*DC Navy Yard Shooting,* 2014), deployed subjects who are unable to be reached (*Safeguarding Our Nation's Secrets: Examining the Security Clearance Process*, 2013), a lack of requirement to obtain a full police report in the first place (*The Navy Yard Tragedy,* 2013), or potential sources' unwillingness to cooperate in the investigation (*Safeguarding Our Nation's Secrets: Examining the Security Clearance Process*, 2013). Miller of OPM, brought out that sources like "employers, neighbors, coworkers, references, etc." do not always cooperate since participation is voluntary, and in some cases, "the best that OPM can do is to make its best effort to locate relevant information through alternative means, and provide notations concerning what is missing" (p. 83). The GAO, however, contends that if documentation as to why an item was not obtained during an investigation exists and is present in the file, then the item was not counted as deficient. Miller, however, disagrees and questions GAO's assessment (*Safeguarding Our Nation's Secrets: Examining the Security Clearance Process*, 2013).

In addition to incomplete information going to adjudications, the overall adjudications category also stressed how important it was to have standards (and to communicate those standards) in order to control adjudications. Although there are supposedly standards in place, as brought out in the "Application" section regarding reciprocity, these standards are often interpreted differently across agencies. Miller states, "Today quality is in the eye of the beholder, depending on the agency, depending on the adjudicator, whether it is complete, whether it is not. So there is a lot of gray area …" (*Safeguarding Our Nation's Secrets: Examining the Security Clearance Process*, 2013, p. 18). As an example, the GAO found that when trying to determine if a case is complete, OPM reviewers, in addition to federal investigative adjudicative standards,

also consider “the unique aspects of each investigation” when deciding adjudication (p. 136). If an individual is deployed and unavailable, then the case is considered complete although it may lack a subject interview. So as evidenced in this case, although there are standards, these standards are open to interpretation.[52]

As discussed in the “Application” section, a problem with standards is also a problem with reciprocity. In order for multiple agencies to trust the favorable adjudication of a BI, the belief is that there should be standard, coherent criteria that guides the process. The interpretation of a completed investigation is an impediment to reciprocity. This is especially evident in the example of the decision if a case being adjudicated is completed or not. Agencies may often have their own idea of what is needed for a completed case, and the interpretations of completeness by an agency are often not communicated between agencies. This may or may not compel an agency to request additional case work. According to the GAO, without agencies sharing information, “agencies may take steps to obtain additional information, which creates challenges to immediately granting reciprocity” (*DC Navy Yard Shooting*, 2014, p. 172). For instance, the DOD sometimes does their own BI work to fill in the gaps for OPM’s deficient reports (*The Navy Yard Tragedy*, 2013), and other agencies may not request any additional information.

The consequences of this lack of communication in adjudications can be seen by Alexis and Snowden’s cases. If the adjudicator working on Alexis’ case considered Alexis’ case, with minimal information on a law enforcement record incomplete, this case may have been returned and subsequently adjudicated unfavorably. According to a House of Representatives executive summary, “Key information sometimes does not reach the agency adjudicators, which means that individuals—such as Aaron Alexis—are occasionally granted clearances that, had the adjudicator been aware of all the pertinent information, should have received more scrutiny and could have

[52] Also of note, even though there may be standards, the standards may not ensure a quality investigation. Farrell brought this up in post-hearing questions for the record when she disclosed OPM’s position that “gathering all the information required by the federal investigative standards does not necessarily indicate a quality investigation"...and that “an investigative report that includes all of the items required by the federal investigative standards does not equate to having obtained the right or best sources of information about an applicant” (*The Navy Yard Tragedy*, 2013, p. 136). Just because boxes were checked regarding the investigative and adjudicative criteria doesn’t mean that that case is a quality case.

been denied" (H. Rep., 2014, p. 2). Additionally, Snowden's investigation failed to look into his security violation at the CIA, and had the adjudicator asked for rework into this, Snowden's clearance may have been impacted (*The Insider Threat to Homeland Security: Examining Our Nation's Security Clearance Process*, 2013, p. 2). Each example shows that the determination of incompleteness is important to the overall adjudication, and if agencies do not agree on what is a completed case, cases can be adjudicated differently thus proving standardization does not exist. Senate Bill 2683 – the CORRECT Act proposes to standardize procedures such as when a case is incomplete, how adjudicators are trained, metrics for oversight of processes, or who is able to unfavorably adjudicate a BI (as recommended, only a federal employee) (S. 2683, 2014).

Overwhelmingly, this section calls for a standardized definition of a complete case as per adjudicative requirements so that there is uniformity in adjudication which will transfer over to uniform reciprocity. Adjudications is an important step of the process because this is where an individual is sorted and granted or denied a clearance. Problems at this stage have great consequences if done incorrectly. However, in the context of the eight categories, it is important to note that "Adjudication" is the second smallest category. This again is especially problematic because this is the step which determines whether someone does or does not get a clearance.[53]

The lack of discussion of this section suggests that the process is blamed more than the adjudicator. If Congress thought that the adjudicator was to blame for a faulty process, then I imagine that there would be more discussion about adjudicators. It is also of note that it was not necessarily the adjudicative criteria (for instance, the use of alcohol) which was contested; it was the completeness of the files. Like the "Application" section, the criteria being used to base decisions off of was not really a topic of concern. More importance was placed on a call for standardization rather than a call to reexamine the adjudications criteria. While this is a very important point, I do not discuss this much further due to the scope of the project. In chapter five I chose instead to focus on the application step because it was the least discussed step (and not

[53] Although a lack of adjudication discussion is an important point to note, due to constraints of the dissertation, this point was not analyzed in-depth.

the second least discussed) of the process. Additional research into this step would be beneficial at a later date.

Appeals

The appeals process does not happen in every investigation, but it does happen in certain circumstances.[54] According to Brenda Farrell at the GAO, the appeals process occurs after a clearance application is denied or when a previously granted clearance has been revoked (*The Navy Yard Tragedy*, 2013). The process varies depending on the circumstances of the disqualification to include agency and appeals processes. As shown in Table 24 below, this category had two major subcategories: 1) Revocation/suspension/appeals and 2) Safeguard for employees. Figure 16 illustrates the category and subcategories. Abridged information for this section is available in Appendix P.

Table 24.

Reforms Needed in Appeals

Appeals Total Entries - 121			
Subcategory / Number of Entries	**Further Subcategories**	**Definition**	**Example**
Revocation/ suspension/appeals - 54	• Contractor and employees • Inconsistent implementation • OPM – Lack of program • Oversight • Punishment • Uniform criteria	There should be uniform procedures for withdrawing someone's clearance.	S. 2683, the CORRECT Act, recommends that there should be "uniform criteria and procedures, consistent with any appropriate Federal Governmentwide standards, including notice requirements,

[54] In the passages, appeals meant that employees were denied a clearance by an agency (USGAO, 2014b), or it pertained to a contracting agency losing a clearance for their business and being debarred from future contracts (Nomination of Hon. Katherine Archuleta, 2013). For the most part though, this section pertained to individuals.

			for the suspension, denial, and revocation of eligibility for access to classified information of an individual issued by the Department" (S. 2683, 2014).
Safeguard for employees - 67	• S. 2683 • Appeal serious actions • Due process • Employees • Inappropriate actions taken • Kaplan v. Conyers • Less safe • Merit Systems Protection Board • Right to counsel • Uniform standards	Processes are not uniform resulting in inconsistencies in clearance implementation that can hurt employees.	"Inconsistent implementation of the requirements …have resulted in employees in some agency components and workforces experiencing different protections and processes than employees in other agency components and workforces" (USGAO, 2014b, p. 23).

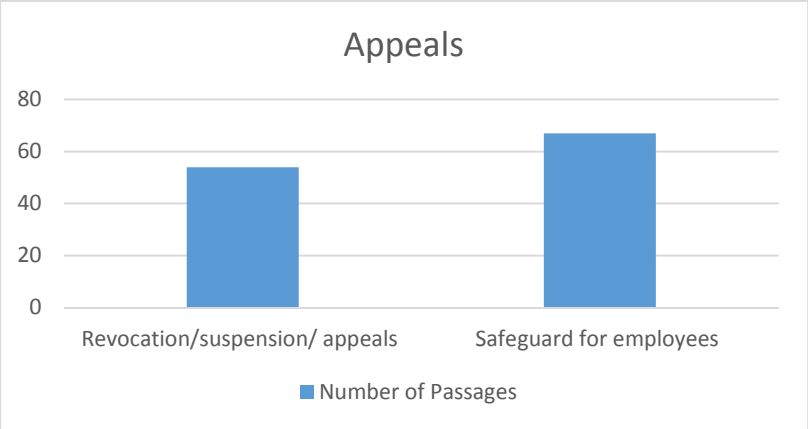

Figure 16. Graphic Results of Appeals Subcategories.

I concluded that the results of the revocation/suspension/appeals and employee safeguard subcategories work together to show that Congress suggests the appeals process is flawed mostly due to inconsistency in the overall process. They also indicate that this inconsistency is problematic because it can lead to problems for employee rights.

The major problem for appeals was a lack of standardization of position designation requirements as previously discussed in the "Requirements Determination" section.[55] A lack of requirements for appeals is a big enough issue that legislation was written to address it. According to Senate Bill 2683, also called "The CORRECT Act", there should be issued "uniform criteria and procedures, consistent with any appropriate Federal Governmentwide standards, including notice requirements, for the suspension, denial, and revocation of eligibility for access to classified information of an individual issued by the Department" (S. 2683, 2014).This includes OPM who has an inconsistent record debarring their own investigators accused of fraud (*Safeguarding Our Nation's Secrets: Examining the Security Clearance Process*, 2013).

Due to a lack of standardization, agencies are able to create their own criteria for determining which positions need clearances and how punishment should be handled in those positions. Due to agency discretion in how clearance matters are handled, how agencies control their appeals process differs across agencies which can lead to inconsistent punishments for similar positions across agencies (USGAO, 2014b). This can result in inconsistences in a right to counsel, reassignment, or termination.

Without standards, there is also a question of oversight. If there are no uniform metrics in place to monitor the procedures, then the government doesn't know if the revocation processes are working to remove the right people from contracts. This is seen by the GAO's statement, "Having assessment tools and performance metrics in place is a critical initial step toward

[55] As a caveat though, some do not treat revocation standardization as a top priority. For instance, the GAO reported that the Office of the Director of National Intelligence (ODNI) who is in charge of national security activities, said "that from an efficiencies perspective, standardization of the security clearance revocation process makes sense, but said that ODNI has not had a reason or purpose to perform an extensive review of the revocation processes" (USGAO, 2014b, p. 40).

instituting a program to monitor and independently validate the effectiveness and sustainability of corrective measures" (USGAO, 2014b, p. 39).

Congress also reaffirms the immediacy of standardized appeals because it is the thought that once a continuous evaluation program is in place, then more people might have their clearances revoked because instead of relying on self-reporting (akin to self-incrimination), continuous evaluation will work to remotely monitor the lives of those with clearances and automatically notify a security office of potential issues (USGAO, 2014b). Because of continuous evaluation, it is "critical for agencies to have a high-quality clearance revocation process in place" (USGAO, 2014b, p. 54).

The other significant theme that emerged in this section concerns safeguards for employees. From the testimony advocating for legislative safety measures, I interpreted some feel that if the government is developing new processes for more monitoring and attempting to standardize procedures, then employees should have safeguards for punishment procedures. For instance, due to the ruling the Kaplan v. Conyers case, "[T]he U.S. Court of Appeals for the Federal Circuit, in a 7–3 decision, held that the Merit Systems Protection Board, lacks jurisdiction to review the merits of executive branch risk determinations regarding eligibility to hold national security sensitive positions before the Merit Systems Protection Board (MSPB)" (*Safeguarding Our Nation's Secrets: Examining the National Security Workforce*, 2013, p. 7). This board formerly allowed hearings of appeals, but with Kaplan v. Conyers, this isn't possible. The CORRECT Act is trying to reinstate this (S. 2683, 2014), but this bill has not yet passed. This lack of appeal is especially concerning considering that there are proposed regulations in the works that would standardize an agency's ability to designate any position as sensitive (*Safeguarding Our Nation's Secrets: Examining the National Security Workforce,* 2013), and as previously discussed according to Colleen Kelley, National President of the National Treasure Employees Union, the designations may not be based on a need for security information; the position

designations could be due to an attempt to get rid of an employee based on race, religion, protected speech, retaliatory reasons, or for whistleblowing (p. 77).[56]

First as a takeaway, the passages in this section overall call for uniform revocation procedures and advocate that employees should 1) retain their right to due process, 2) retain their right to counsel, and 3) be treated fairly. Second, it is interesting to note in this section the differences in the way contractors and federal employees are discussed. Although the two may be doing the same job, because their employers differ, the discussion of their treatment also differs. For instance, according to Senator Tom Coburn, "When Federal employees are suspected of falsification, they are placed on administrative leave until the case is resolved and evidence is gathered to support being fired, while still getting paid. Contractors are immediately removed from contracts" (Nomination of Hon. Katherine Archuleta, 2013, p. 81). The difference shows how adamant the concern is for the fair treatment of employees and the lack of concern for the contractors. Showing up in other passages, the ability to fire contractors immediately is discussed as one of the benefits of maintaining a contractor workforce (*The Navy Yard Tragedy*, 2013, p. 110). This shows up again in the deductive category dealing with surveillers. The status of government contractors is similar to the status of adjunct faculty in academia. Both groups are treated differently, and anecdotally, the contractor and adjunct as inferior to the full time employee by not receiving the same benefits of working full time for the institution. While the cachet of the contractor will not be discussed more fully in this dissertation, I feel that situation is problematic and is addressed only for the wrong reasons in the Congressional documents. The documents discuss more the monetary cost of the contractor and question the quality of their work rather than question the working conditions contractors face as addressed by Davenport (2015). Summarizing this overall though, this section does call for more standardization and employee protections.

[56] An individual could be found as no longer suitable for his/her position due to increased suitability criteria due to an increased security designation level. The Congressional documents did not provide any specific examples of this happening though.

Periodic Reinvestigation

Anyone holding a clearance is subject to the reinvestigation process, and during this phase, the individual holding a clearance undergoes the appropriate background investigation to make sure they still meet the qualifications for the clearance (*The Navy Yard Tragedy,* 2013). According to Stephen Lewis, Deputy Director for Personnel at the DOD, the current requirements for a Top Secret clearance review is five years, and at the Secret level and below, clearances are every ten years (*DC Navy Yard Shooting*, 2014). This could be longer though due to backlogs and agencies not submitting paper work on time (S. 113-283, 2014).

There were two emergent categories in this section: "More/continuous Evaluation" and "Time Between Investigations." The two categories overlapped but still remain distinct. The first subcategory is a call for more assessment and is a result of subcategory two's problems of too much time elapsing between evaluations with only self-disclosed checks and balances in between. Table 25 below provides the further subcategories, definition of the category, and an example text. Figure 17 is a graphic representation of this information. Abridged details of this category are listed in Appendix Q.

Table 25.

Reforms Needed in Periodic Reinvestigation.

Periodic Reinvestigation Total entries - 183			
Subcategory / Number of Entries	**Further Subcategories**	**Definition**	**Example**
More/continuous evaluation - 138	• Definition • Drawbacks/ Limitations • Frequency • History • How it works • Programs • Real time • Role of Tech • Why used/ justification - generic examples • Why used – specific examples	Those with clearances need to be continually (and not just periodically) monitored.	"It is this whole issue of continuous evaluation, and, whether it is the 5-year cycle or the 10-year cycle, this is to me the critical issue that we are missing" (*The Navy Yard Tragedy,* 2013, p.35).

Time between investigations - 45	• Current • What is wanted • Who set the 10 year time • Why	Time between investigations allows problematic behavior to proceed without repercussions.	"Well, because there is a 10-year interval between investigations, that information [Alexis' law enforcement activity], unless it became known to the commander or supervisor of Mr. Alexis, would not have been reported to the Department of Defense" (*DC Navy Yard Shooting*, 2014, p. 53).

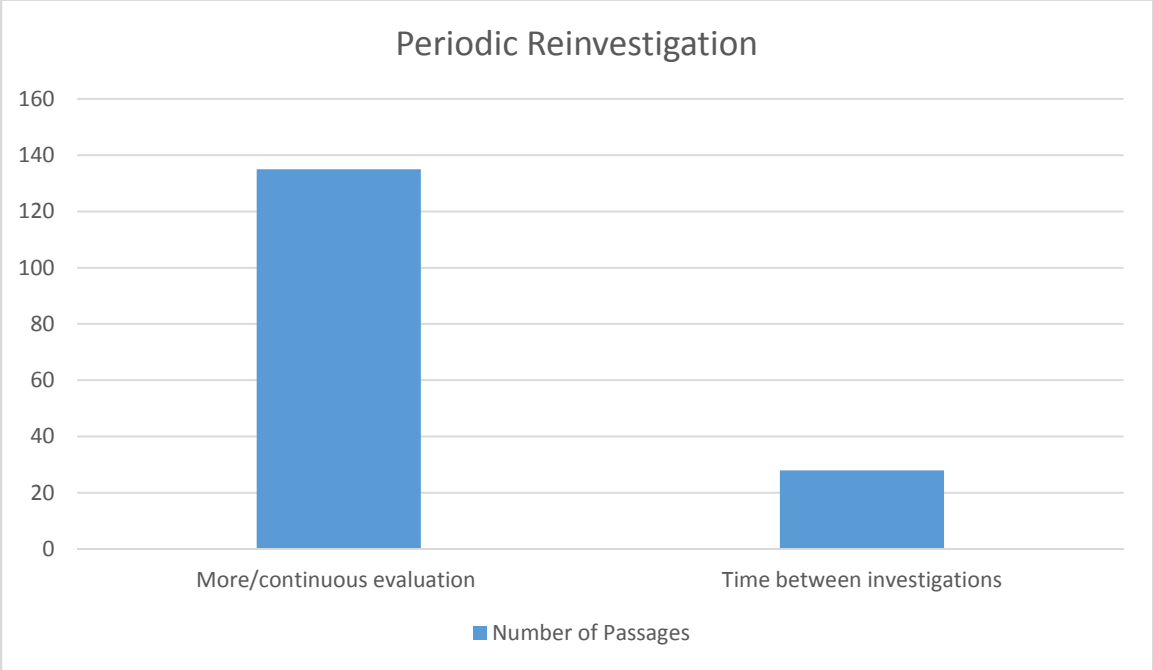

Figure 17. Graphic Results of Periodic Reinvestigation Subcategories

The largest subcategory in this category involves calling for more/continuous evaluation and is driven by the desire to get more information on subjects of investigation on a more frequent basis. The call is in the form of a specific initiative called "continuous evaluation" which will supplement a previously existing "Insider Threat" initiative. [57] According to the Senate,

[57] The "Insider Threat" initiative is a product of Executive Order 13587 signed in October 2011 which sought "to complement the continuous evaluation concept by incorporating data from a

continuous evaluation “means reviewing the background of an individual who has been determined to be eligible for access to classified information at any time during the period of eligibility” (S. 2683, 2014). This process hopes to close the gap between investigation times (H. Rep., 2014) as well as eliminate the ability for individuals continue to hold a clearance after an adverse action because they did not self-report this event (S. 113-283, 2014; *The Navy Yard Tragedy,* 2013).

The call for a continuous flow of information is justified by belief that there is too much time between investigations. The US Senate reports, “The current reinvestigation practices do not adequately reevaluate or appropriately mitigate risk within the security and suitability population. Lengthy periods between reinvestigations do not provide sufficient means to discover derogatory information that develops following the initial adjudication” (S. 113-283, 2014, introduction). Because of these gaps between investigations, Congress suggests it is imperative to shorten time between these investigations. According to OPM’s Archuleta, continuous evaluation is needed “so that we are getting this information not once every 10 years, but we are continually provided information about anyone who holds a secret or top secret clearance” (*DC Navy Yard Shooting*, 2014, pp. 64-5). Without these extra checks, the passages discuss that incidents such as Alexis will happen again (S. 113-283, 2014). Additionally, had Alexis’ BI checks occurred more frequently and not relied on self-admitted information, Alexis may have lost his clearance before he was able to murder coworkers at the Navy Yard (*DC Navy Yard Shooting*, 2014).

There was pushback on the idea of continuous evaluation though. First, the documents were cautious about protecting employee rights when calling for the gathering of more information, and text from the Senate Bill 2683 included that “standards for the protection of national security and promotion of fairness, transparency, and employee protections, including safeguards to preserve the rights and confidentiality of whistleblowers” should be included in the

---

broad set of data sources to identify problematic behavioral trends will help identify those that need to have clearance or authorization revoked” (*The Navy Yard Tragedy*, 2013, p. 225). The Insider Threat initiative is not discussed further in this dissertation as it was initially issued in 2011 and outside of the scope of the research questions. For more information, please see http://www.ncsc.gov/nittf/docs/ National_Insider_Threat_Policy.pdf .

adoption of any new program (S. 2683, 2014). Regardless of this though, Congress is still interested in putting continuous evaluation in place.

Also, just because continuous evaluation is a goal of Congress for BIs, that doesn't mean it is necessarily possible, and there have been several criticisms of the program. First, similar programs have been attempted in the past. According to Senator Portman, the DOD talked about supposedly going to use the Automated Continuous Evaluation System (ACES) and have it in place by 2005 (*The Navy Yard Tragedy*, 2013). However, by 2013, Stephen Lewis of the DOD testified that it "is still in a research and development mode" analyzing about 3,600 of approximately 2.5 million people (p. 37). Problems with the process occur because continuous evaluation "adds significant cost and resource burdens to federal agencies and to the federal adjudicators" (p. 100), and problems also occur due to a question of having the staff available to evaluate this information (p. 169), a question of how this information is evaluated, and a question of how agencies can "take action based on that information" (p. 37). This reflects similar concerns of OPM's Merton Miller when discussing using social media content in BIs (*Slipping*, 2014, pp. 37-8).

Additionally, a continuous evaluation system for all clearances has technological limitations. For the DOD and ACES, Lewis continues that "One of the things we are examining is can we expand the capability of the system to handle that larger volume. And that is a work in progress…" (p. 37). For a larger continuous evaluation program overall, the same problems exist. According to the verbiage of the Enhanced Security Clearance Act of 2014:

> Implementing a system for continuous evaluation is resource intensive, and poses genuine technical and procedural challenges. Currently there is no government-wide capability, plan or design present in the investigative community to operate a data-driven architecture to collect, store, and share relevant information. (113-283, 2014)

Further, the volume of information is greater with automated checks, and "[a]lthough these pilots have identified actionable information, they indicate that retrieving, analyzing, and processing the data is likely to be resource intensive" (*The Navy Yard Tragedy*, 2014, p. 65). So, overall although continuous evaluation may seem like an answer to "inefficient and resource intensive" checks, that doesn't mean it is easy to accomplish.

The difficulties in integrating this system can really be seen by 2016, and this is the largest takeaway from the "Periodic Reinvestigation" section. Several bills introduced to Congress attempted to solidify continuous evaluation as a common practice. Senate Bills 1618 and S. 5482 (both called the Enhanced Security Clearance Act of 2014), S. 2683 and H. 5240 (both called the CORRECT Act), H.R. 4022 (called the Security Clearance Reform Act of 2014), and H.R. 490 (called the Security Clearance Reform Act of 2015) all discussed implementing some form of continuous evaluation. Each wanted to go about instituting a program that would allow continuous monitoring of governmental employees. The hope was that this would involve using governmental and commercial data sources (S. 113-283, 2014), automated records checking (*The Navy Yard Tragedy*, 2013), and specifically "access Federal, State, and local government and commercially available information, including financial credit history, currency transactions, court records, traffic violations, arrest records, terrorist and criminal watch lists, foreign travel, and online social media" (H.R. 490, 2015). It was also the hope that this information would be pushed in a real-time capacity and shared between all agencies with enterprise-wide technology so that every agency, and especially the clearance granting agency, would be aware of an individual's transgression (*The Navy Yard Tragedy*, 2013). Further, H.R. 490., S. 1618 and S. 5482 specifically called for certain cleared individuals to be "subject to two randomly timed audits every five years" (S. 113-283, 2014).

As time has passed however, it is interesting to note that by 2016 none of these acts have passed. The last movement on any of these bills was on H.R. 490 when it was referred to the Subcommittee on Crime, Terrorism, Homeland Security, and Investigations on 2/19/15. Nothing further has come from the other bills, and it appears they died in Congress in 2014 (Henderson, 2015b). So, with time and actions in hindsight, while Snowden and Alexis jumpstarted a conversation on BIs, of the acts discussed in the documents reviewed for this study, only the Score Act (S. 1276 and H.R. 2860) regarding oversight for the IG (as discussed in the oversight section) have passed. While continuous evaluation is a goal, it may not be plausible at this current time.

Miscellaneous

As originally shown in chapter three, Table 4 is repeated here as Table 26 and provides the subcategories of the miscellaneous section. The passages in this document either provide background information about specific stakeholders or processes outside of the research questions or present themes not directly looked for through the lens of the research questions. I included these passages and grouped them into subcategories because of either their role in defining what some of the larger themes entailed (e.g., steps of a security clearance) or because they provided a picture of another theme that seemed significant but did not fall under the results of BIs directly. Some themes may have shown up within the passages, but they were not separated for the merit of their own worth. For instance, the steps of the clearance process have appeared throughout the dissertation, but they weren't isolated by themselves. I wanted to keep track of these themes because they could provide additional spaces of analysis for additional research, but they did not address the research questions of the current study.

Table 26.

Miscellaneous Results

Background Information	Miscellaneous Themes
• Costs • Definitions • OPM's Role • Physical security • Steps of a clearance process • USIS • What clearances do • Who has a clearance	• Feelings about the BI • General distrust of BIs • Liberties/Freedom • Privacy • Trust • Whistleblower

Before discussing the takeaways, I'll briefly discuss each category by starting with the "Background Information" side. The "Costs" subcategory does not show problems associated with costs, but rather this section specifies the costs of the investigations. For instance, a passage states, "the Executive branch spends over $1 billion dollars on background investigations for suitability and security clearances" (*The Insider Threat to Homeland Security*, 2013, p. 1). The "Definitions" subcategory functions as a dictionary for some of the main topics included in the research. For instance, periodic investigations are defined as "investigations conducted

periodically, with a frequency as required by the Director of National Intelligence, for the purpose of updating a previously conducted security background investigation" (S. 113-283, 2014). The "OPM's Role" subcategory details what OPM does for the BI process and beyond in government. For instance, according to S. 13-111 (2013), "OPM is tasked with managing the federal workforce in a variety of ways, working with government agencies and employees on issues from recruitment to the resolution of labor disputes." The subsection on "Physical Security" is interesting because it is related to BIs because often to get into a facility one needs a clearance, but facilities themselves also undergo a process similar to individuals in that a facility gets investigated as to its risks and necessary security matters. For instance, "Risk assessments (facility security assessments) are the foundation upon which an effective facility security policy is built" (*The Navy Yard Tragedy*, 2013, p. 228).

As previously discussed, the "Steps of a Clearance Process" details what goes into conducting a BI. Although several charts discussed in this dissertation provide an overview of the process, these passages detail the processes in writing. For instance, "The scope of the background investigation is dependent upon the level of the security clearance required" (*The Navy Yard Tragedy*, 2013, p. 11). The USIS section provides specific details about USIS not necessarily associated with the problems it caused to the BI. For instance, "USIS is the single biggest contractor that performs background investigations for the Office of Personnel Management, completing more than the Government or any other contractor" (*DC Navy Yard Shooting*, 2014, p. 3).[58] The "What Clearances Do" subcategory focuses on the functions of clearances and sketches out the role of clearances. For instance, Brenda Farrell of the GAO states, "Personnel security clearances allow for access to Classified information on a need-to-know basis…and to be granted access to certain government buildings" (*The Insider Threat to Homeland Security*, 2013, p. 23). The final subcategory "Who has a clearance" provides a summary of the number of individuals that have a clearance. For instance, Representative Peter

[58] In 2015, Altegrity, the company that owned USIS, filed for bankruptcy.

King states that “the Department of Homeland Security has over 120,000 employees with a security clearance” (p. 1).

The first subcategory in the Miscellaneous Themes” side is “Feelings about the BI” and discusses how those with clearances and in the government feel about clearances such as Senator “Heidi” Heitkamp’s feelings that “when we give them the Good Housekeeping Seal of Approval, which is what this security clearance is, that ought to mean something” (*The Navy Yard Tragedy*, 2013, p. 32). The “General Distrust of BIs” section addresses the idea that regardless of how BIs are conducted, they aren’t going to be fool-proof. For instance, Gregory Marshall of the DHS states, “I need to make clear, however, that security aims to manage risk, not eliminate it” (*The Insider Threat to Homeland Security*, 2013, p. 12). The “Liberties/Freedom” section has passages suggesting that more oversight may cause problems for liberties and freedom such as when Senator Tester states, “As we move forward, it is critical for us to examine the scope of these programs to determine whether they properly balance our security and our essential liberties” (*Safeguarding Our Nation’s Secrets: Examining the Security Clearance Process*, 2013, p. 1). The “Privacy” section also addresses concerns of privacy such as when Susan Ordakowski of KeyPoint (another government contractor) comments that, “[i]t is important, however that the utilization of such sources [social or traditional media] be balanced against a person's right to privacy” (p. 34). The “Trust” section addresses an implicit trust of the BIs and is counter to the idea of a general *distrust* of BIs. Passages here suggest that the BI is trustable and can be fixed. This section does not show up in under the research questions analyzing the problems of the BI since it is not indicating problems but rather trust. For instance, Representative Gerald E. Connolly suggests that although there was formerly a backlog of investigations, due to Congressional action, “in an example of good governance that has become all too rare these days, the security clearance reform efforts worked” (*DC Navy Yard Shooting*, 2014, p. 149). The final subcategory of “Whistleblower” looks at the way whistleblowers are constructed in the documents such as a pro-whistleblower comment from Canterbury of POGO that states, “We must be able to hear from whistle-blowers” (*Safeguarding Our Nation’s Secrets: Examining the National Security Workforce*, 2013, p. 13).

In all these results, I felt the most important takeaway in this section was the emergence of a flawed understanding of BIs (outside of the context of the Federal government). I noticed that there was a difference between a distrust for the current Federal BI process and a belief that BIs themselves are adequate in general. Differentiating these two threads was important to my study and influenced the final conclusion that people fundamentally trust BIs in general. Due to the importance of this category, I laid out every subcategory in Table 27. These categories together undercut the whole BI process and ideas of reform. While Congress works to fix the problems that exist in the current federal process, these passages demonstrate that there is a fundamental inability to predict the future or eliminate all risk from a system. Of note, it is interesting that over 1/4th (7/25 or 28%) of general passages come from report #28 about facilities (*Facility Protection*, 2013). This leads me to hypothesize that when actual physical locations are breached,[59] that is when the argument that BIs are not perfect seems to emerge. The resistance to the BI as THE method of screening will be discussed further in chapter five when addressing the implications of my study.

Table 27.

General Distrust of BIs beyond the Federal Process

Reason	Definition	Example
Can't eliminate risk	No matter how good BIs are, they can't eliminate all risks.	"I need to make clear, however, that security aims to manage risk, not eliminate it" (*The Insider Threat to Homeland Security*, 2013, p. 12).
Can't find everything	BIs can't find everything regardless of trying.	"It is important to note that any background investigation, no matter how rigorous, is no guarantee that all relevant information is known, available, or has been included" (*The Insider Threat to Homeland Security*, 2013, p. 12).
Can't predict the future	BIs aren't able to predict the future.	"Even those who have successfully undergone the most rigorous set of background checks available--even a comprehensive polygraph examination--may someday prove

[59] It is interesting to note that there was no discussion of digital breaches. While, for example, Snowden and Manning were responsible for the spread of information digitally, this was not the focus of the congressional documents.

		untrustworthy" (*The Insider Threat to Homeland Security*, 2013, p. 14).
Only look at past	BIs really only offer a look at the past.	"Ultimately, a Federal background investigation only examines past behavior and is sometimes based on limited available Information" (*The Insider Threat to Homeland Security*, 2013, p. 14).
Bureaucracy always systemic	The BI problems are an issue of bureaucracy and not process.	"I want to make it very clear that this is not a problem created by this Administration; this is a problem of bureaucracy, longstanding, but no longer can we stand for it" (*DC Navy Yard Shooting*, 2014, p. 2).

Category One Summary

Overall, there were many passages that made up this category. The passages discussed the BI process in general, covered oversight of the process through things like standardization and metrics, and broke down the problems at every step of the process. Each of these recommendations worked to show how the BI process is failing and what can be done to fix it. Although, as the miscellaneous section illustrated, there was some pushback to the abilities of the BI, for the most part, the BI was assumed to be a process that can work and can be "fixed."

Results of Deductive Study

The second research question addressed looking at the congressional reports through the terministic screen of surveillance studies. As I have established, in the previous chapters, the documents were viewed deductively through eight categories: 1) constancy; 2) surveillant assemblage; 3) surveillers; 4) sorting; 5) risk; 6) prediction; 7) identity, and 8) technology. In the following section I give a brief overview of each category in order to illustrate how the documents fit the idea of surveillance and illustrate how applying another terministic screen changes the interpretation of the Congressional communication. In chapter five, I then look at the implication of these connections. Abridged details of each section are available in Appendix A, B, and D-I. Figure 18 shows a brief overview of where the passages relating to themes of surveillance matched up the most. In the appendixes, I show the passage number for each subcategory, but I do not illustrate the breakdown in the body of this dissertation because this would be irrelevant for

my study as I did not draw any conclusions based on the subcategories of this section. I only focus on the eight larger categories for my conclusion in chapter five.

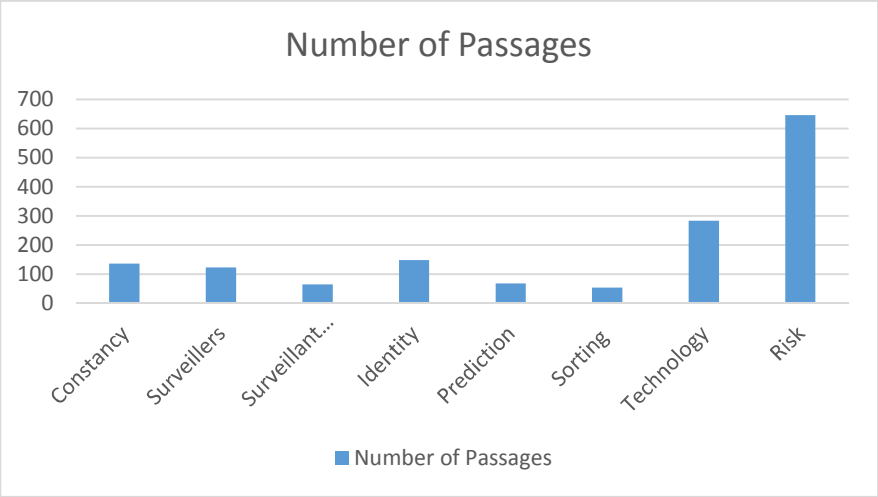

Figure 18. Passages related to surveillance

Constancy

I found that the BIs had reflected the contemporary surveillance characteristic of *constancy*, and I classified one hundred thirty-six passage sections into this category. As described in chapter two, a position surveillance studies holds is that surveillance control comes in the forms of continuous assessment (Deleuze, 1995, p. 182). Surveillant practices take in information about a population continuously, and "constant monitoring checks worker activities and individual inducements provide incentives for compliance" (Lyon, 2007, p. 60). For the purpose of this dissertation, the filter of constancy was used to identify places in the BI reform documents where control was illustrated by practices of continuous monitoring.

The results for the "Constancy" section showed that there is an attempt by Congress to continually monitor those that have a clearance by electronic means such as through databases in order to make sure these individuals are still fit and able to hold a clearance under the BI standards. Called *continuous evaluation* (CE), this term is even semantically similar to the phrase *constant monitoring* that Lyon used above. The CE program is designed to deliver almost real-time results of adverse actions such as arrests, and it can supposedly help prevent a catastrophic

event such as Alexis' murderous actions. Congress suggests that had Alexis been subjected to continuous evaluation, his troubles with the police would have been discovered, possibly making him ineligible for a clearance (H. Rep., 2014). Results of the places where constancy shows up in the congressional documents category are listed in Table 28. The primary subcategory for this category is "Continuous Evaluation," and under this subcategory, the data from the congressional reports was further broken into eleven subcategories.

Table 28.

Topic Results for Constancy

Constancy -136
• Continuous evaluation o Definition o Drawbacks / Limitations o Frequency o Gap between investigations o History o How it works o Programs o Real time o Role of tech o Why used/justification – generic examples o Why used – real examples

The section of constancy is one of the more direct overlaps with the first question which used inductive methods and the categories emerged from the content. More, and continuous, evaluation was the answer to many of the problems Congress put forth and many of the bills introduced in this time advocated initiating this continuous evaluation program (H.R. 490, 2015; H.R. 4022, 2014; H.R. 5240, 2014; S. 113-283, 2014; S. 2683, 2014). It is interesting to note though that although the inductive results championed the idea of continuous monitoring, someone like Snowden who disclosed classified information because he believed the government was conducting too much surveillance might see continuous monitoring as not a solution but as another problem.

Breaking the passages down in the lens of surveillance studies helped flesh out the relationship between surveillance and the BI. While the idea of continuous evaluation may appear

to be just a reaction to the gap between reinvestigations which causes inconsistency in self-reporting, the pairing of the congressional documents with surveillance studies shows that the initiative is actually part of a larger fundamental shift in our ideas of surveillance and control. Surveillance can be seen as shifting to near constant monitoring, and because these digital languages transcend institutional site, one can never really leave the institution. For the government, continuous evaluation may be a safety measure to make sure individuals are living clearance-worthy lives (as the government has defined clearance-worthy), but for those with a clearance, the practice of constant evaluation places them under constant control. Some may argue that if there is nothing to hide there is nothing to fear, but it is naïve to think that constant surveillance doesn't have consequences. Surveillance produces a type of subject (think Foucault's docile bodies), and for one example, theories on intellectual privacy illustrate that people should be allowed freedom to think, and when they feel they are being surveilled, the surveillance causes people to not to experiment with new ideas (Richards, 2013).

Surveillant Assemblage

As I discussed in chapter two, a control society is different from a disciplinary society. In a disciplinary society, regulation is more aligned with being under direct supervision of one central entity. In a control society, we are monitored by a variety of sources which may just watch a slice of our lives such as loyalty cards, Department of Motor Vehicle records, Netflix viewing histories, or Google search terms. Surveillant assemblages are thus the variety of sources gathering this information and the variety of data which the surveillance accumulates. Because a variety of sources may be providing information (often in digitized form), the information may be seemingly disparate and only gains meaning when it is by whatever institution is reassembling the information.

BIs correlate to this characteristic of surveillant assemblage. Investigative information is gathered by investigators (and a variety of investigators – either contractors or federal agents) from a variety of sources, and reassembled in a number of locations. BIs themselves thus become assemblages that are gathered from disparate sources and reassembled by OPM. While the agency in charge of the investigation holds the most power and ultimately decides who gets a

clearance, power is still found in multiple places from the difference data gathering sources. To illustrate, according to Prioletti of the ODNI:

> "One of the obvious sources, potential sources of information, is social media or publicly available electronic information. What I referred to in terms of the research was the idea that we need to look at both what possible sources of information are out there, which ones would be of most benefit to provide adjudicatively relevant information for the access to classified information…" (*The Navy Yard Tragedy*, 2013, p. 40).

This passage alludes to a collection of distributed information from different sources which have power over groups of people which can be used for governmental ends.

BIs can thus take on characteristics of assemblages: they allow fluid "systems of domination" where power is asymmetrical and entities are able to control others (Haggerty & Ericson, 2000, p. 206). For instance, speculatively, if Prioletti had his way, those undergoing BIs may be at the mercy of their Google searches. If an applicant has searched something the government deems problematic, then the applicant could be questioned about that search because a Google history could be included in the information included in the BI. In ways that may have been previously considered a private activity (suspending disbelief that searching the Internet has ever been truly a "private" activity), Google may be able to maintain power over the applicant in ways that may not have existed with more limited and centralized sources of information.

Table 29 illustrates more fully the comparison of the congressional passages to surveillant assemblage. I categorized sixty-five passage groups into this category and concluded that the emergent themes could be grouped into three subcategories, each broken down more inductively in one further subcategory. Additional information appears in Appendix G.

Table 29.

Topic Results for Surveillant Assemblages

Surveillant Assemblage - 65

• Expanded collection, agency, and scrutiny
  o Multiple sources of information
• Multiple locations
  o Locations
• Power not limited to place
  o Reciprocity

In this table, I composed the "Expanded Collection, Agency, and Scrutiny" subcategory with passages that discuss the idea that seemingly unrelated data is gathered from multiple sources and used for control (Haggerty & Ericson, 2000) by employing a variety of techniques such as methods from the military or marketing (Lyon, 2007, p. 95). The "Multiple Locations" subcategory dealt with surveillance information being reassembled in databases in multiple places (Gates, 2011), and the "Power Not Limited to Place" subcategory dealt with the idea that power to conduct surveillance and gather information about someone isn't limited to one place (for instance reciprocity allows power to be transferred from agency to agency).

By pairing the congressional documents with surveillance studies, I saw that the documents also fit the characteristics of surveillant assemblage. I was able to point out the difference between the government doing surveillance and other non-governmental entities providing information for surveillance purposes. By doing this, I uncover that in the inductive results, reaching out to additional agencies like those in the private sector seems to be a natural progression. Collaborating with the private sector is just a way to make BIs better (*Safeguarding Our Nation's Secrets: Examining the National Security Workforce*, 2013). However, when paired with surveillant assemblage, by splitting up power between different agencies and in different places, power becomes distributed and my information is stored in different locations by multiple stakeholders. While this split may not be bad in and of itself, it does lead one to question the privacy policies and information management of the multiple parties involved in providing and assessing surveillance information. It also highlights the difficulties in standardizing surveillance practices since stakeholders are distributed.

Surveillers

As discussed in chapter two, there is no longer just a view of surveillance where surveillance is carried out by a totalitarian state like in *1984* (Orwell 1949/1950) or watching in a confined, institutionalized, fixed location like in the Panopticon (Foucault, 1977). Instead, information comes from multiple sources in various locations. This information is reassembled in databases (Gates, 2011) in places like law enforcement facilities, financial centers, Amazon or Netflix facilities, or at Google. In contemporary surveillance then, surveillers are not just state

actors and come from a variety of locations in positions which may or may not have been traditionally associated with power (i.e., a loyalty card now controls information on the shopper, but a supermarket may not be a traditional wielder of power).

In the breakdown of the data, I determined that the results for the "Surveillers" section had one hundred twenty-three passages and returned one subcategory: different surveillant agents, and this section could be broken down in two other subcategories as listed in Table 30. The passages in this section were guided by the idea that in today's surveillance, "[o]ld lines [of control] become blurred – lines that once distinguished police work from private security, or law enforcement from consumer management" (Lyon, 2007, p. 107), and the passages results were split between contractors and employees doing the surveillance. I did not break down this section further than contractors and employees into more distinctions of where the information came from for the BIs such as Google as was discussed in the "Surveillant Assemblage" category. I did not do this because for the BI in particular, I considered technology was more of a *source of information* rather than an entity in charge of doing the surveillance. For this section, I chose *surveillers* to mean those directly conducting the investigations. For the BI, a human element would review information from technology.

Table 30.

Topic Results for Surveillers.

Surveillers - 123
• Surveillant agents o Contractors o Employees

For conducting the BI, the overall substance of this section was that contractors and employees both conduct BIs, and using the language of surveillance studies, I could consider this to mean older surveillance practices using traditional government resources are blurring. For instance, the GAO illustrates the multiple agents when they state, "Investigators—often contractors—from Federal Investigative Services within the Office of Personnel and Management

(OPM) conduct these investigations for most of the federal government using federal investigative standards and OPM internal guidance as criteria for collecting background information on applicants" (*DC Navy Yard Shooting*, 2014, p. 154). Before 1996, BIs were considered inherently governmental activities. That year, the Clinton administration privatized part of OPM's workforce and created US Investigation Services (or just "USIS"), and since then, both contractor and employees have conducted the BIs (Barr, 2003). Although few passages allude to the government origins of USIS, in the almost twenty years after privatization, in 2013, USIS was no longer closely aligned with government and owned by a private equity firm. Passages further talk about other contractors like KeyPoint and CACI and show how the work is shared between OPM and the contracting agencies (*DC Navy Yard Shooting*, 2014). Overwhelmingly though, the documents address how both contractors and the government are working together to conduct BIs. I did not include technology or private industry in the "Surveillers" category even though they might provide surveillance information because essentially, it is only contractors or employees using technology or information from private industry, and for BIs, contractors and employees are the agents assembling and conducting the BIs.

As a caveat though, in this "Surveillers" section (like results in the "Appeals" section), it was relevant to note the number of passages used to negatively differentiate between contractors and employees. For instance, the contents of the Security Clearance Reform Act of 2015 creates a distinction and divide between contractors and government when it calls for only federal workers to conduct "any final quality or integrity assurance review…any interview of a covered individual with respect to a background investigation; and…any background investigation of a covered individual to determine the person's eligibility for a security clearance at the Top Secret level or higher" (H.R. 490, 2015). The Act's verbiage thus indicates that only government employees are qualified agents to conduct many essential functions of the BI. Additionally, as shown in the inductive category results looking at the problems of the BI, the quality (*The Insider Threat*, 2013) and value (*Safeguarding Our Nation's Secrets: Examining the Security Clearance Process*, 2013*)* of the contractor workforce is often called into question, and some in Congress think that contractors are not held to the same standards as employees (*The Insider Threat*,

2013). Interesting to note too is that as shown by the "Appeals" section, employees had more chances to protest accusations of wrongdoing (even despite some losing MSPB appeal rights). Contractors are often immediately terminated while employees are often put under investigation and given due process (Nomination of Hon. Katherine Archuleta, 2013).[60]

Overall though, despite that clear distinctions are often drawn between the government employee and contractor, this section does show that the difference between government and non-government workers is often hard to determine, and government workers are not always the agents conducting seemingly governmental functions. I think that the recurrence of the distinction between the two types of employees is beneficial to monitor because of the real differences between government employees and contractors,[61] but to fully address the distinctions was not in the scope of this dissertation. For surveillers though, there were clear examples that emerged in this dissertation that illustrated the government is not the only agent conducting surveillance.

Social Sorting

As discussed in chapter two, social sorting often concerns using searchable databases in order to provide differing levels of service for different groups of people (Lyon, 2009). A Netflix viewer only watching comedies may be sorted into the category of "comedy watcher." Similarly, an individual with bad credit history may be sorted into the category of someone who shouldn't get a loan. In each case, one's data was used for differentiation purposes and to categorize the individual as one thing or another. Especially in the case of the individual that did not get a loan, the sorting could have caused a negative impact on his/her life.

---

[60] Senator Claire McCaskill adds to the narrative of both a muddied division between government and non-government workers but also maintains the divisions when she states, "All through our government there has been an easy way to augment personnel by doing these program support contracts, and at one point in time, and probably still at Homeland Security, you could not tell the contractors from the employees. They were doing the same functions. They were sitting at the same desks. They were working on the same things. One was a contractor and one was not, and partly it was because supposedly they were easier to get rid of" (*Safeguarding Our Nation's Secrets: Examining the Security Clearance Process*, 2013, p. 27).

[61] For instance, according to the *Washington Post*, OPM employees and contractors have different productivity standards (a point system versus man hours), and contractor measurements may force increased productivity pressures to meet corporate revenue expectations (Davenport, 2015).

I categorized the fifty-four representative passages from congressional reports for social sorting into three subcategories, each further broken down in one additional subcategory. Table 31 lists the results of the section. Additional abridge information is listed in Appendix F.

Table 31.

Topic Results of Social Sorting

Social Sorting – 54

• Databases
  o Adjudication
  o Difference between crimes
  o Sorting as tool for acceptance/denial
  o Tech
• Codes
  o Facilities
  o Law enforcement
• Consumer surveillance
  o Credit use

The passages in this section focused on texts that discussed databases used to categorize individuals. For instance, according to text from the Enhanced Security Clearance Act of 2014, an enhanced security review "must integrate relevant information from various sources, including government and commercial data sources, consumer reporting agencies, and social media, including the types of information that are relevant for consideration in a background investigation" (S. 113-283, 2014). The passages also looked at the idea that since information is inputted in a database, the computerized/coded version of an individual is often used to determine access. An example of this is found in a House of Representatives report. The passage discusses cases with no issues which OPM and the DOD calls "zestfully clean," and to determine if the individual should get a clearance, "a computer reviews the file and has the ability to grant the clearance; since there is nothing for the first-level adjudicator to review, no such review takes place" (H. Rep., 2014, p. 30). In this passage, not only is an individual's life put into a database in order to determine a clearance, a computer is actually making the decisions on whether to grant or deny the clearance. This is especially interesting in light of the previous discussion detailing how the government does not want contractors making this decision because

determining clearances is an inherently governmental function, yet in these cases, a computer is doing it.

By combining the theory of social sorting to the congressional documents, the juxtaposition highlights the function of the BI to create categories of haves and have-nots: those that are sorted favorably get a clearance, and those that are sorted unfavorably do not get a clearance. The more sociological spin on the function of the BI in regards to sorting makes me stop and evaluate the decision-making results of the BI. Social sorting's emphasis on the disadvantages that sorting produces is important to look at because it can result in problematic determinations. For instance, as already discussed in the "Requirements Determination" section, employees can be deemed ineligible to hold their job "based on incomplete or faulty background information…for reasons motivated by an employee's race, religion, or constitutionally protected speech…for retaliatory reasons… [or] because the employee is a whistleblower" (*Safeguarding Our Nation's Secrets: Examining the National Security Workforce,* 2013, p. 77). Additionally, as shown in the "Investigation" section, using credit information as a determining factor if someone should get a clearance employs thinking that "financial hardship equates to disloyalty" and is offensive (*Safeguarding Our Nation's Secrets: Examining the National Security Workforce*, 2013, p. 10). Sorting really highlights that there is not necessarily a bad or good, but a set criterion someone has created that supposedly translates to safety or risk, regardless as to the reality of those designations. This section raises the concerns that the criteria used to determine eligibility really needs review, such as the application and adjudications steps of the BI where the government determines what information needs to be gathered and what criteria will be used to evaluate an applicant's fit for a clearance. As this dissertation has shown though, problematically, these two steps are the least discussed processes in the discourse of the BI reform.

Risk

As discussed in chapter two, risk is a constructed idea that identifies what elements may threaten a society. Risks are bad things that could happen, and risks should be managed to be mitigated. For instance, if society thinks gun violence is a risk, then guns might be banned through legislation because guns are seen as a threat. Conversely, if instead a society feels that

it is more of a risk to be without guns, then gun control would be a threat and there would be attempts to stop such legislation. Either way, risks should be avoided, and there are elaborate systems in place to control and prevent risks from occurring.

I put the results from the "Risk" section into three subcategories, each broken down inductively in multiple, further subcategories as listed below in Table 32. Appendix E shows additional abridged information. Important for chapter five's discussion, "Risk" was the largest categories of information because, after conducting the study, I concluded the results show that the BI is basically an exercise in risk management. The government tries to control risk and forecast the future with BIs. Supposedly BIs can identify and hopefully eliminate from consideration those that look like they pose a threat to the government and classified information.

Table 32.

Topic Results of Risk.

Risk – 647		
• Types of risks o Adjudicative guidelines o Alcohol o Association o BIs o Can't get all o Communication o CE o Credit o Damage potential o Derogatory info o Documents missing o Drugs o Education o Employment o Facilities o Foreign o Inside threats o Internet o Law enforcement o Lifestyle o Mental / emotional o Prohibited items	• Risk communication systems o Adjudication o Director of National Intelligence (DNI) o Determination of clearance o Facilities o Investigator o Level o OPM o Problems o Reciprocity o Rules, regulations, laws o Steps of a clearance	• Basis for assessment o Access to food supply o Adjudications decide suitability o Alcohol o Citizenship o Conduct o Dishonesty is bad o Drugs o Employment problems o Financial problems o High-risk individuals o Law enforcement o Mental health o Need identity

o Residence o Sources o Subjects o Terrorism o Under-reporting		

The BI identifies and communicates risk, and through its various process, it defines what can supposedly threaten society. The subcategory “Types of Risks” identified the risks that supposedly identify a risky individual. For instance, when discussing why the information might be valuable for the BI, Merton Miller from OPM stated, “In fact, postings of people drinking when they were under age might be on the Internet” (H. Rep., 2014, p. 37) signifying that underage drinking is a risk factor. Other types of risk showing up in the results are use of alcohol, associations, drug use, foreign contacts, mental health, and many others. The subcategory “Risk Communication Systems” concerned the laws and regulations which govern the process. The GAO provides an example of process when they comment, “DHS and DOD can revoke an employee’s eligibility for access to classified information based on 13 adjudicative guidelines” (USGAO, 2014b, p. 10). The “Basis for Assessment” section contained passages identifying what is used to justify not granting a clearance. For instance, Elaine Kaplan from OPM stated that failing to report a serious event “is certainly grounds for revoking a security clearance, and failing to report or being dishonest when you fill out your form is something that the adjudicator would take into consideration in deciding whether to grant a clearance in the first instance” (*The Navy Yard Tragedy*, 2013, pp. 30-1). Some of the same results show up from the first subcategory and the third subcategory, but the third relates more to how these factors are related to one’s identity: it is the difference between a risky person rather than a person engaging in risky behavior. The risky person may seem to be fundamentally a risk, and the person engaging in risky behavior may be seen as safer but participating in risky activities.

Comparing the “Risk” section to the inductive results shows that the criteria used to determine if one is eligible for a clearance is really just an assortment of constructed variables which supposedly identify the factors that make an individual a risk. Risk, in a constructionist view as described in chapter two, does not represent a capital “T” truth; it is often just what has been identified by one group to be a risk. Whether or not these identifications of risk really are a

representation of the variables that identify potential problems is a discussion for a further study, but at this point for this study, it does draw attention to the constructed nature of risk and its associated risk communication systems.

Prediction

As discussed in chapter two, prediction deals with using surveillance to predict events before they occur. Using algorithms or other measures such as an analysis of crime statistics or presence of undesirable adjudication traits such as bad credit, if there is a probability that an individual may deviate from desired behavior (i.e., he/she has divulged classified information rather than keep it secret), then the individual is considered a risk and may not get the advantage of whatever they are trying to obtain.

I put sixty-eight entries in the "Prediction" section and categorized the results in three subcategories, each broken down in multiple, further subcategories as listed below in Table 33. Appendix D shows additional abridged information.

Table 33.

Topic Results of Prediction.

Prediction – 68		
• How to predict o Alert o Continuous evaluation o Credit o More people, more risk o Processes o Random o Warning Signs/ Flagging/ High Risk Designations	• Technology and Prediction o More technological monitoring = prediction	• Probabilities and Prediction o Belief in prediction o No belief in prediction o Only past account – skeptic

The first way I categorized the passages in the "Prediction" section was under "How to Predict" which was grounded by the surveillance studies idea that the purpose of surveillance is to reduce individuals to code in order to be socially sorted for prediction. For instance, Zureik (2003) indicated that surveillance goes from observation to prediction by using statistics to infer

profiles, and the subject is deconstructed and not directly under scrutiny (p. 39) which helps to explain Staples (2000) comment that "[d]ata generated through surveillance techniques produce 'types'" that are at "risk" for behavior (p. 6). An individual is observed, turned into code in a database, and then compared to others in the database to determine "types." In this sense, prediction can apply not just to the individual but to an aggregate group of individuals. To illustrate this idea, if I claimed that millennials are most likely to default on a loan,[62] then anyone that was a millennial may get an extra layer of scrutiny when applying for funds because they are categorically and statistically apt to default. As an example of this from the documents I reviewed, according the GAO, there is a separation code that any military personnel are coded as they leave the military. These codes make them eligible and ineligible for things such as security clearances (USGAO, 2014b). Depending on the code, the individual will get more or less scrutiny.

The second subcategory "Technology and Prediction" discusses that surveillance relies on technology to help predict the future (Gates, 2011; Graham & Wood, 2003; Jewkes, 2004; Kim, 2004). An example of this is Representative Peter T. King's comment that "[o]ne potential element of the Insider Threat Program is the use of analytics to identify and even predict potential breaches of information systems based on an individual's pattern of system access" (*The Insider Threat to Homeland Security*, 2013, p. 49). In this sense, technological analytics are ideally going to identify problem behavior before it occurs.

The final subcategory in this section is "Probabilities and Prediction" and discusses the idea that risk communication systems focus on "calculating probabilities" (Lyon, 2007, p. 38), and if it is probable an event could happen, then the event can be predicted and prevented. For instance, the text of the Enhanced Security Clearance Act of 2013 reads, "The OPM Background Investigation process must be capable of flagging high-risk individuals holding clearances and alert case officers of situations requiring review before any adverse consequence takes place" (Enhanced, 2013). This shows that individuals labeled as "high-risk" become probabilities and need to be stopped (or at least watched with more scrutiny) before they create problems.

[62] This is just an example and not based on any research.

This section does, however, also contain passages that complicate this idea. For instance, Gregory Marshall of DHS comments, “Ultimately, a Federal background investigation only examines past behavior and is sometimes based on limited available information” (*The Insider Threat*, 2013, p. 14). This idea has been previously discussed in the “Miscellaneous” section concerning a distrust of the overall process. Just because a BI has been completed, and perhaps even completed well, this doesn’t mean that the BI can accurately predict what someone will do in the future. Further, as Scott Stewart (2013) states, BIs are just focused on outward indicators of problematic behavior and fail to really examine deeper insights into the character of applicants. BIs do not necessarily predict what an individual will do in the future.

So overall, this section on risk not only shows that the identification of risks helps shape prediction, but this section also creates a dialog that questions the whole process and abilities of the BI. This makes the idea of prediction central to the doubt that arises from the BI and its ability to be “fixed” using the Congressional recommendations.

Despite the complications, I think the overall the takeaway from this section is the awareness of the hope in the predictive capabilities of the BI. As shown though, prediction is not only problematic because of the socially constructed criteria that is used as a basis to determine who is a risk, but it is also problematic because often an individual may just be lumped in a category of people who are presumed to be at risk even though the individual may not be of risk personally. And because technology is involved, then the individual may just be a statistic or unit of code filtered into a have or have-not category. For instance, as shown above, high-risk individuals supposedly have a high-probability of doing something bad. They may be lumped into the “bad” category. Also an opposite example, as shown in the social sorting section, in cases of “zestfully clean” cases (H. Rep., 2014, p. 30), these individuals have not set off any probabilities of risk, and they are so inconsequential a computer gives them a clearance. Each may in reality pose a threat, but each are filtered and lumped into categories which supposedly indicates a *probability* of risk and not and absolute assurance of events to come.

Identity

As discussed in chapter two, identity deals with the constructed nature of identities and the idea that identities really only emerge in certain contexts (Barnard-Wills, 2009, 2012, & 2014; Lyon, 2009) often related to the preferences of those using the data and not related to a preexisting identity. A more accurate term too for how others feel about us is *identification* (Lyon, 2009). The idea of *identity* is how we define ourselves; identification is what is ascribed to us by others. For instance, the data double or the code used to socially sort us becomes our identification. Our identity is who we think we are.

The results from the "Identity" section resulted in six subcategories, each broken down in multiple, further subcategories as listed below in Table 34. Appendix B provides further abridged information.

Table 34.

Topic Results of Identity.

Identity - 148		
• Articulated in context o Adjudications o Changeable o People don't agree with determination o Whole person	• Obsessed with checking IDs o Facts Exist o ID Card o ID Cards revoked for derogatory info	• Ascribed by institutions o Government-defined identities o Identity based on adjudication
• Biometric ID o Fingerprints o ID	• IDs are self-generated and revealed information o Public info and social media o Self-reporting o SSNs	• Basis for assessment (also in risk) o Access to food supply o Alcohol o Adjudications o Citizenship o Conduct o Dishonesty o Drugs o Employment o Financial problems o High-risk individuals

		o Law enforcement o Mental health o Need firm identity

The passages in this section started with the subcategory “Articulated in Context.” This section dealt with the idea that identities are relational, always involve others, and always change (Lyon, 2009, p. 12). The second subcategory was “Obsessed with Checking IDs” and involved passages that discussed using a physical from of ID as a way to determine identity. The third subsection “Ascribed by Institutions” dealt with passages that saw identity as socially constructed and dependent on the place. The fourth subcategory was “Biometric ID” and contained passages discussing places on the body that are used for identification. The fifth section “IDs are Self-Generated and Revealed Information” contained passages discussing public information, social media, and self-reported information for use in the BI. This information can be seen as identity information used by identification purposes; an individual reveals things about him/herself, and then this information is used by others for identification. The final section was “Basis for Assessment” which also has to do with risk, and this section contained passages showing how risky behavior becomes part of an identity profile in the case of BIs.

Overall, the passages in this section reaffirmed that identity is something that emerges from specific places and is not a universal, unchanging essence of who we are. These subjective identities are then used to sort us into categories. Illustrating many of these positions is the following passage from OPM’s Merton Miller. He states, “The decision that an individual should receive access to Classified information is ultimately, pursuant to Executive Order 12968, the exclusive responsibility of the head of the agency employing the individual, or his or her designee, following a National security adjudication (either by that agency or by a central adjudicative facility working on its behalf)” (*The Insider Threat*, 2013, p. 9). This comment shows that identity is ascribed by an outside entity based on executive orders and adjudications criteria. The decisions either grant or deny access to sensitive information and are built on someone else’s interpretation of us and not from some unwavering core of who we are.

Putting identity in context of the congressional passages shows how constructed identification is, and although one may feel they have a particular identity, for the BI, it is really other institutions that ascribe an identification to them. An individual becomes fit for a clearance depending on how much they deviate from the prescribed adjudications criteria (which, as shown previously, is socially constructed and currently relatively uncontested).

This section also really emphasizes the problematic phrase "whole person" that appears throughout the passages. Congress asserts that the BI's "whole person" assessment is "made by utilizing the whole-person concept, which is a careful weighing of available, reliable information about the person, past and present, favorable and unfavorable" (*The Insider Threat to Homeland Security*, 2013, p. 16) which paints the picture of an unbiased evaluation, but put in conversation with the other surveillance variables of sorting, risk, and prediction, I can conclude that an unbiased evaluation is not possible. The whole BI process is built on institutionally defined variables that are not without bias. And it is essentially the agency who decides who an individual is through identification rather than an acceptance of an individual's identity. The identification is imposed from above while the identity is a more self-constructed sense of self.

Technology

As I discussed in chapter two, technology in this section deals with the use of technology such as databases and algorithms in surveillance and the implications that technology has on the process of monitoring and controlling a population. It helps explain the change in surveillance data collection and ties the major surveillance themes together. Technology facilitates continual monitoring, helps store data for surveillant assemblages, becomes a partner to the surveiller, conducts social sorting through algorithms, keeps track of risk and identifies patterns to the future, and helps assign identities through sorting.

I divided the "Technology" section (with two hundred eighty-three passages) into five subcategories, each broken down in multiple, further subcategories as listed in Table 35. Additional abridge information is available in Appendix I.

Table 35.

Topic Results of Technology.

Technology - 283	
• BIs using tech o Accuracy o Automation o Collection o Continuous evaluation o Control o Cost o Database o Delivery o Duplication o Enterprise-wide /database o Exclusion o Internet/social media o Paper o Programs o Reliability o Sharing o Solution o Tools o Unrealistic o Web-based	• Tech and biometrics o Automation o Continuous evaluation o Database o Enterprise o Fingerprints o Program
• Confinement and exclusion o Keeping in / keep out	• Everyday use of tech o Public and social media

The first subcategory was “BIs Using Tech.” This section contained passages discussing how the BI process involves technology and was guided by the idea that technology turns physical and observable information into code (Zureik, 2003) which is then stored electronically and can then be searched through databases (Lyon, 2003b). For instance, there is guidance from Congress that agencies should report information to multiple repositories of clearance information such as JPAS, CVS, and Scattered Castles which will help with sharing information and reciprocity (*The Navy Yard Tragedy*, 2013). These systems link clearance profiles so that agencies can tell who has a clearance and thus can be further monitored remotely and thus use technology to communicate the coded body.

The second subcategory was “Tech and Biometrics” and had passages which address the use of technology to gather biometric data. For instance, according to US House report, “FBI fingerprint and name databases identify whether an applicant has been arrested in the United

States" (H. Rep., 2014, p. 16). This passage shows how fingerprint data, from the body, is used to gather and monitor the clearance-seeking individual.

The third subcategory was "Confinement and Exclusion," and this section contained passages related to the idea that surveillance technologies serve two functions: 1) confinement (fencing in) and 2) exclusion (fencing out) (Bauman & Lyon, 2013). An example passage from this section is from OPM's Miller when he states, "OPM did create a position designation tool that was focused on suitability and determining what type of level of investigation is required for the position in question" (*Safeguarding Our Nation's Secrets: Examining the Security Clearance* Process, 2013, p. 20). This passage, along with pretty much the entire purpose of the BIs, represents the idea of fencing in and fencing out. Based on determinations of clearances and levels of clearances, individuals may or may not access information.

The fourth and final category is "Everyday Use of Tech" which looks at the use of public and social media information desired to be used in clearances and is motivated by the surveillance theories that power circulates digitally and surveillance is embedded in our daily actions through things such as technology (Deleuze, 1995; Lyon, 2007). For instance, Senate Bill 113-283 calls for more access to public electronic information, and goes into more details of what that means. The bill states "publicly available electronic information" includes:

> relevant security or counterintelligence information on any social media website or forum, that may suggest ill intent, vulnerability to blackmail, compulsive behavior, allegiance to another country, change in ideology, or any other information that may suggest the covered individual lacks good judgment, reliability or trustworthiness; and (E) data maintained on any terrorist or criminal watch list maintained by any agency, State or local government, or international Organization. (S. 113-283, 2014)

As discussed in the "Identity" section, people could also use social media in order to reveal things about their identity that the BI uses for the purposes of identification, but it is of note to remember that this is dependent on technology such as the Internet, databases, and algorithms to construct and sort profiles. Without technology, there may not be the same amount of self-disclosure. An example of the use (or desired use) of social media is from a House report which is advocating for the use of social media information and states, "These three social media and search sites [Twitter, Facebook, and Google], among others, contain a treasure trove of

information about their users. And the Americans that hold, or will apply for, federal security clearances use them frequently" (H. Rep., 2014, p. 36). This passages illustrates the hopes that technology will help supplement other investigative tactics. Additionally, as a side point, the idea that it is "a treasure trove" further illustrates that Congress thinks there is lots of information available on the Internet that is somehow not being included in the BI (thus the words "treasure trove"), and this does further complicate the idea of the "whole person" that is somehow not including a "treasure trove" of information. Additionally, identifying what pieces of information are relevant to a BI is also a matter of interpretation (Young, 2015), and as discussed in the paragraph below, the logistics of actually using this information would be difficult.

By incorporating this discussion of surveillance technology into the discussion the larger conversation of BI reform, this section highlights the role that technology plays in the entire process of BIs. Technology is used to assist in investigations, adjudication, communication between agencies, and to monitor the whole process. Of note though, just as in the first section using inductive methods, this section also resulted in the admission that technology can't solve everything, and often too much faith is put into technological answers (such as the discussion on continuous evaluation). For instance, Representative Blake Farenthold commented that when trying to devise a new system, the federal government does not have a good track record with other large technological programs. He stated about the hopes of credit score automation, "It seems like that is something that could, at a very simple level, be automated. You have their name, you have their date of birth, you have their social security number. Okay, after Healthcare.gov, I am questionable about the Government's ability to automate anything or compute its way out of a paper bag" (*DC Navy Yard Shooting*, 2014, p. 61).

Additionally, Miller of OPM stated about the Internet:

> So I think right now the real keys have been is everybody sees it as a potential lead development tool, but not a tool to be used for investigative purposes because of the potential privacy issues, number one. And then, from my perspective, it's the analytics that would be required behind the information you collect. For example, having worked counterintelligence operations, it's one thing collecting information. It's a whole other process, more costly, to verify the veracity of that information and then connect the dots. So I could, as you could, you could go out and build an Internet persona for me tonight. You could go home and say, Miller, you know, put that out there, and all I would have to do is do a search and I would see what you wrote. Now, so what is the veracity of that

> information? You wrote it. You posted it. Somebody is going to have to determine the reliability of that. So that's the hard part, I think, in applying the social media role in background investigations. (H. Rep., 2014, pp. 37-38)

As Miller brings out, social media can contain a lot of unreliable data. Sometimes the site's norms can even call for playful or exaggerated information that could be misinterpreted in the context of a BI (Young, 2015). Further, many times people use the internet to troll for reasons varying from entertainment purposes to more serious character implications like sadism (Maltby et al., 2016). The investigator would need to take into account the truthfulness and reliability of what was said and weigh how representative of character online comments really are. However, I would argue this examination seems more fit for academic study than in the context of a BI which results in social sorting.

Overall though, both passages complicate the idea that the government can be helped by technology. The passages suggest that the government will automate credit scores or incorporate Internet information but also question that the government can do this due to previous precedence with Healthcare.gov and problems with veracity in identifying what is accurate on a social media page.

With these complications too, I have my own reservations about the fitness for incorporating technology into the BI. Technology is not always an asset, and this is very evident in the OPM data breach from the summer of 2015. According to *The New York Times*, over 21.5 million people had their information possibly exposed when hackers (the US government blamed China) breached OPM databases allowing access to sensitive information about those subjected to a clearance, their relatives, and their friends (Hirschfeld Davis, 2015). In this case, technology assisted in hurting the very same people that clearances are supposed to protect. Although an examination of which type of damage would be worse for an individual – a leak of state information by a cleared employee or a leak of personal information by the government, is an important matter for debate, due to the scope of this dissertation, I won't explore this issue further.

Despite this complication of the value of technology though, overall this section brings up the use of technology when doing surveillance and the reliance on technology, searchable databases, and self-reported data for the purpose of BIs.

Category Two Summary

Combining all eight categories of constancy, surveillant assemblage, surveillers, social sorting, risk, prediction, identity and technology brings another level of depth to the overall Congress' discourse. These categories, all inter-related, work to destabilize the normalization of the recommendations that Congress makes to "fix" the BI process. Whether it be constant monitoring, collecting information from a variety of non-governmental places by governmental and non-governmental actors, socially sorting those with a clearance into categories based on risk for the purpose of prediction and identity determination made possible by technology, these surveillance studies understandings show that the recommendations are not just unbiased, value-free solutions but rather processes embedded in surveillance constructed by those who are in power. This power has the ability to produce the haves and have-nots, so this process needs to be questioned at every step.

Conclusion

Overall, by comparing both categories, I concluded that for the first section, Congress has a lot of unbridled optimism when adding more surveillance for BI safety. The majority of suggestions for BI improvement encourage more surveillance especially in the form of continuous monitoring and oversight. It is interesting too though that much of this surveillance also involves more surveillance of those involved in carrying out the BI process such as OPM as an agency, adjudicators, and investigators in the form of more standardization, more oversight, and more training.

Conversely, the second section that used inductive methods sees those same passages in a more skeptical way. While the first section showed these passages as a solution, the second section used the same passages as supporting evidence for surveillance practices. For instance, constant monitoring was a solution for Congress, but constant monitoring can be problematic for

surveillance studies. Using the passages in this way demonstrated that by taking another perspective on the subject, the surveillance practices that are normalized by Congress become problematic when viewed in through surveillance studies. The suggested reforms can become evidence of a problematic construction of identity by government and non-governmental actors which obtain surveillance information from a number of sources (again, both government and non-governmental) using technology to establish identification for the purpose of sorting individuals based on risk and the important result of prediction which may or may not be accurate and complete, perhaps on a continual basis. And despite that the government says they use "the whole person concept" in adjudications, this whole person is really constructed based on biased notions of risk (such as those with credit problems have probabilities of selling classified information to get out of their debts)[63] that really don't encompass a whole person specifically since they work on identification rather than identity. The "whole person" is how an adjudicator would see an individual not as the individual under investigation would see themselves.

For this study, I interpreted the passages as suggesting that identities can be constructed, the future can be predicted, and technology can make things easier. While there may be truth to some of these claims, for the most part, the passages spent little time questioning the fundamental reliance on a process (and the socially constructed application or adjudication steps) seemingly believed to be unfailing. Because some people with clearances did problematic things, these individuals supposedly "slipped through the cracks." However, these cracks may not really exist because there isn't in existence an infallible system in the first place (Young, forthcoming). Actions such as Snowden and Alexis may just be acts which can't be explained by a bad BI. They may just be illustrations of the lack of ability to predict the future and not necessarily a call for more surveillance. BIs may not be all that they are supposed to be, and looking further into the normalization of these processes should be the goal of those involved in the process. I will address this faith in the BI further in chapter five when I compare the two

[63] It is interesting to note that Dr. Mike Gelles (2001) of the Naval Criminal Investigative Service notes that "spies value money not just for what it can buy, but for what it symbolizes – success, power, and influence." It would seem to make sense then to also focus on one's view of money in addition to just identifying a need of it. This idea is not in the scope of this dissertation, however.

discussions from this chapter together to examine the implications of applying another terministic screen to the Congressional communication.

CHAPTER 5

DISCUSSION

To review, my dissertation looked at congressional documents advocating BI reform since Edward Snowden divulged classified information in June 2013. Chapter one introduced the study and my research questions which asked, 1) based on evidence from congressional hearings, bills, daily editions, and reports, since Congress began to react to Snowden's disclosures in June 2013, what arguments have emerged in the documents as flaws to the BI process? and 2) how does applying another terministic screen change the interpretation of the congressional communication? In chapter two, I situated my research with a discussion of rhetoric and the terministic screen, surveillance studies, and BIs. I sketched out the methodology of my study in chapter three, and in chapter four I provided the results of my research. I found that there was a call for more surveillance in the form of more standardization and continuous monitoring, and I also found that of principles of surveillance complicated the theories behind the "solutions" that Congress offered. For instance, ideas such as constant monitoring, confirming identity, and the benefits of more technology, when viewed through the lens of surveillance, aren't necessarily all possibilities or positive solutions. Constant monitoring can change the way people think, identities are problematic (especially when ascribed by positions of power), and technology can cause problems for BIs (such as a leak of 21.5 million individuals' sensitive information). In this chapter, I summarize the study and discuss the implications of my results.

In order to determine the largest implication for my study,[64] I decided to identify what Congress looked at both *most* and *least* in their documents, or essentially Congress' terministic screen.[65] This allowed me to see both what Congress was focusing on and what they were turning their attention away from. After looking at the results of both questions, I found that the *application* was the least discussed step of the BI process and idea of *risk* showed up the most.

[64] There were many implications that could be drawn for this study, but I wanted to focus on one or two in order to provide depth for at least some areas.

[65] As Burke (1984) stated regarding the terministic screen, "Every way of seeing is also a way of not seeing" (p. 70).

Congress thus turned their attention most towards notions of risk, but they also turned attention away from the application. Putting both together, Congress reaffirms that the BI is a way to manage risk, but they proportionately neglect to address the application, a step which is integral to the BI process. Of what was discussed for the *application* step, the focus was predominantly a generalized push to standardize the BI applications, especially for the purpose of reciprocity so that agencies can honor each other's BIs. There was little discussion of exactly *what* should be standardized.

A lack of attention to the content of the BI application and this step in general in the context of risk is what I consider the most important implication of this study, and this conclusion is of special importance due to the scientized way the BI gathers information in a risk communication system. The form can be a scientized procedure because it turns the application into a replicated system which produces uniformity and closure. For my study, this replicated system is risky because if little attention is given to the application itself, then the questions the application asks and data the form generates can, 1) lead to national security and social justice risks because the form continues to uniformly gather possibly irrelevant information; and 2) the continual replication of the procedure without analysis also reinforces a sense of closure that once a certain series of questions are asked, then the BI is completed and risk is minimized, providing a potentially false sense of security and overconfidence in the BI.

Lack of Form Attention

To expand, after putting all the results of study together, as shown in the last chapter, the passages indicated that Congress overwhelmingly called for more BI standardization, more types of surveillance, and more frequent evaluation. As indicated in chapter four and supported by the abridged Tables in the appendix, this is largely what I found with the data. What I could not find though, and what I think is the larger implication to come out of this study, is that of all the categories of recommendation, the least discussed step of the BI process was the *application*. There was little Congressional interrogation into the questions and assumptions that the form

requests of its users.[66] Figure 19 originally featured in chapter four illustrates this lack as it shows just how few passages I attributed through my analysis to being considered in the applications section.

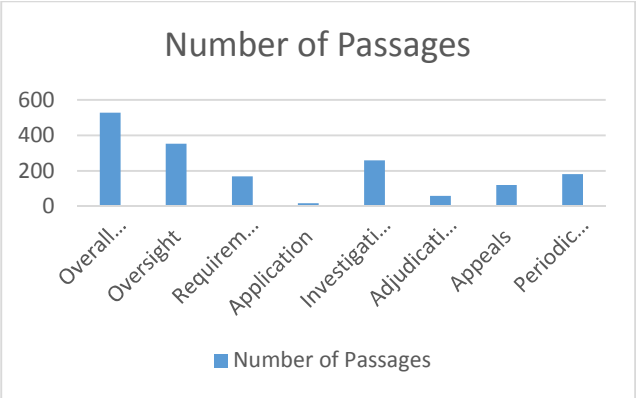

Figure 19. Graphic Representation of Inductive Methods.

Of what I coded "applications," the attention was spent on asserting that the processes should be standardized to ensure reciprocity, but there was no clear discussion of what the standardized procedures would entail and little mention of the form on which the investigation is based. For instance, although ODNI's Brian Prioletti called for the overall reform of the SF-86 for "accurate information pertinent to today's security and counterintelligence concerns" (*The Navy Yard Tragedy*, 2013, p. 67), and Senator Johnson told his anecdotal story of John Hamre's troubles filling out his SF-86 form only in his opening statements as an attention-grabbing introduction, neither really elaborated on their positions. There was no substantial follow up or debate about the comments that would examine the basic application forms. *What* would be standardized was not a topic of discussion.

[66] I think it is important to add that in addition to my dissertation's results, there is not just a lack of attention in *Congressional hearings* for the application step. The processes have largely been neglected even outside of the study results. The SF-85P hasn't been updated since September 1995, the SF-86 since December 2010. Additionally, these updates are still based on the basic principles of the clearance process as set up in 1953 (Defense Personnel Security Research Center, 2005). Even back in 1997, it was reported that the BI process is out of date and should be brought up to date from its Cold War origins (Moynihan, 1997).

Risk Communication

When paired with the literature on surveillance, risk, on the other hand, was the *most* discussed theme. As shown in Figure 20, there were six hundred forty-seven passages that I recorded in the risk category. I concluded that the prevalence of passages in this category occurred because that the BI is basically a way for the US government to minimize risks. BIs are conducted to try to stop adverse actions from happening.

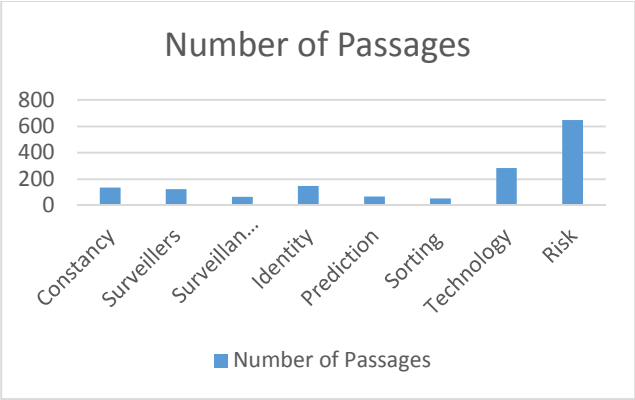

Figure 20. Deductive Category Results.

The problems that can result from the lack of discussion on the application in its function as risk management are best seen through work in risk communication systems as discussed by Ericson and Haggerty (1997). Their book, *Policing the Risk Society*, analyzed law enforcement communication, and they looked at communication formats in which police officers and other department personnel write. The two concluded that the formatting and the way in which communication is organized has “profound implications” on communications and on the agency of the officers involved in constructing knowledge through report writing. Ericson and Haggerty (1997) cite Giddens (1984) who states, “Formats are metacommunication statements, or rules for the recognition, organization and presentation of information and experience” (as cited in Ericson & Haggerty, 1997, p. 31) and Altheide (1995) who concludes, “As the logic of the format pervades the everyday routines and conversations of the workplace, the terminology, metaphors and the imagery of format permeate language and human and idle time” (as cited in Ericson & Haggerty, 1997, p. 31). Ericson and Haggerty (1997) conclude that through formats, police work is “structured by the categories and classifications of risk communication and by the technologies

for communicating knowledge internally and externally" (p. 33). In this sense then, forms help produce discourse[67] and provide the terministic screen through which knowledge is subsequently produced and filtered.

Through their research, the authors stress the impact of institutions on how knowledge is produced, and they find that police work is not situational or based on officer autonomy as Manning (1992) suggested. Instead, the conclusions an officer draws are based on the formatting parameters provided by the institution through which the officer is operating in and relayed through medium like standardized forms. Officers are urged not to think for themselves and are instead required to translate their actions into "institutional, expert-knowledge renderings that establish the route for satisfying those needs" (p. 36). Forms and the rules written about these forms guide the officers to action. The institutional standards embedded in the communicative documents thus define how information is composed and what conclusions can be drawn. Knowledge[68] is further created by combining the forms and data gathered.

Further, the form is a unifying document that gathers information is a uniform way. Thus, the forms allow for the scientization of the work. Ericson and Haggerty (1997) liken an officer to social science field workers that go out into the field with "forms, manuals, and coding instructions" in order to gather data, and police supervisor are like research associates who "cleanse data to ensure that is reliable and valid" (p. 383). The form allows for information to be compared to other information gathered in order to draw larger conclusions through standardization.

While Ericson and Haggerty were specifically talking about the law enforcement agencies, the conclusions that Ericson and Haggerty form are meaningful outside of justice

---

[67] According to Ericson and Haggerty (1997), "Discourse is the institutional construction of knowledge within a social organization of territories, material objects, people, rules, formats, and technologies. What are constructed are representational frameworks: classifications and categories that stand for objects, events, processes, and states of affairs in the world. These frameworks provide the basis for shared understanding…" (p. 83)

[68] Ericson and Haggerty (1997) used Daniel Bell's (1985) definition of knowledge and stated, "Knowledge is interpretation in context, exegesis, relatedness, and conceptualization, the forms of argument" (as cited in Ericson & Haggerty, 1997, p. 84).

studies. For this study in particular, their research is especially pertinent because, 1) for BIs, OPM investigators *are* authorized in law enforcement activities, so already, the BI is closely related to police work. Investigators carrying out BIs, while not law enforcement, are listed as series 1810 in the government classification system which falls under the larger category of the 1800 series, or the Inspection, Investigation, Enforcement, and Compliance Group (U.S. Office of Personnel Management, 2011). While BI investigators don't carry a weapon and are not involved in criminal procedures or enforcing laws, they do fall under the same general umbrella as government law enforcement positions. Additionally, 2) the research that Ericson and Haggerty draw on doesn't just come from police-related research. Among several disciplines, sources such as the aforementioned Giddens (1984) and Altheide (1995) have roots in studies of risk and media. The work that they do thus extends beyond just studies of policing. It borders social science, communication, surveillance, and communication formats across disciplines.

The BI Form

According to Ericson and Haggerty (1997), police forms fit into a rule system which provide "precise communication rules regarding how to format their request for knowledge from informants, witnesses, and suspects…" (p. 322). Further, rules are "embodied and embedded in these forms" which "affect how the police think and act." The forms also tell officers what they must ask, and "[t]he knowledge available in a report depends on the format used and therefore is always secondary to the format" (p. 357). The officers thus adopt the speech and behavior that is required of their institutional discourse. As Ericson and Haggerty (1997) put it, "The communication formats provide the means through which the police think, act, and justify their actions" (p. 33).

One of the main communication formats for the BI is the Standard Form (and all the variations of the form such as the SF-86, SF-85, SF-85P). This series of forms lists questions and provides the subject matter for which investigations are based off of. To be more specific, based on the determined level of sensitivity, an applicant will submit answers to a questionnaire designed to lead the process of investigation (USOPM, "Questionnaire for National Security Positions," n.d.; USOPM "Questionnaire for Public Trust Positions," n.d.). These questionnaires

often come in two formats (although both have variations): the Standard Form (SF) 85 (or the SF-85P[69]) and the SF-86. The SF-85 form is used for public trust positions[70] (U.S. General Services Administration, n.d.) or non-sensitive positions (Federal Clearance Assistance Service, n.d.) and is less comprehensive than the SF-86 which is used for national security and public trust positions. Both forms ask for basic identifiers such as name, date of birth, place of birth, social security number, citizenship, and telephone number. The forms also ask for residential information, education and employment histories, information about references and family, foreign travel, prior investigations, police record, drug use, and finances. The SF-86 form asks for similar but more questions, often for longer durations and for more in-depth information. Additionally, as one answers "yes" to certain questions, the level of depth of information the form asks for increases. For example, question 26.3 on the SF-86 form asks for an elaboration of admitted tax debt (USGAO, 2013, p. 18). If one were to answer that they either failed to file or pay their taxes, then the individual would be required to specify details such as the year of the debt and the amount of the tax debt.

Outsiders to the process can infer which questions may be considered an issue by the additional questions that are asked when an affirmative answer is given. For instance, drug use, alcohol use, certain mental health counseling – all of these areas ask for more information if an applicant checks yes to related questions. The questions which require elaboration can further be paired with the list of adjudications criteria in order to determine why an element from the form is considered an issue. In the case of tax debts, this would be demonstrating financial considerations. The US Government Accountability Office provides the criteria for adjudications and listed the following adjudicative markers:

- allegiance to the United States;
- foreign influence, such as having a family member who is a citizen of a foreign country;
- sexual behavior;

[69] The SF-85P is for Public Trust positions (USOPM "Questionnaire for Public Trust Positions," n.d.), and the SF-85 is used for Non-Sensitive positions (USOPM "Questionnaire for Non-Sensitive Positions," n.d.).

[70] Figures 2 and 3 describe the federal security/suitability clearance process and a describe the investigations.

- personal conduct, such as deliberately concealing of falsifying relevant facts when completing a security questionnaire;
- financial considerations;
- alcohol consumption;
- drug involvement;
- emotional, mental, and personality disorders;
- criminal conduct;
- security violations;
- outside activities, such as providing service to or being employed by a foreign country; and
- misuse of information-technology systems. (USGAO, 2013, p. 32)

Each of the criteria that the application defines as a risk helps define who should be sorted into the *have* and *have-not* categories. These classifications are not necessarily bad, but need attention. As Bowker and Star (1999) state, "Each standard and each category valorizes some point of view and silences another" (p. 34), and sorting is both an ethical but dangerous action. In the case of the BI, if the form asks for credit, then it is defining credit as a national security risk. If the form asks for foreign family members, the form is defining foreign family members as factors contributing to national security risks. The investigator then is required to think through the space that the form outlines and conducts the investigation with the belief that these matters are issues. Depending on the investigative results, an individual with these risks may or may not be considered suitable for access or a clearance. Ultimately then, the form helps define and standardize risk, and in this case, it controls the way BI stakeholders think.

Further, the form is a unifying document that gathers information in a uniform way, allowing for the scientization of the work. The data is gathered in routine ways through an institutional framework to allow for disciplinarily standardized and accepted interpretations. All variations of the Standard Forms have the same questions, and they are designed to have investigators and other security personnel compile data in the same way. The data turns into science when it can be studied and assessed, in relation to similarly gathered information, with a specific (in this case institutional) lens.

According to Ericson and Haggerty (1997), there are at least two outcomes to having the data gathered in a uniform, scientized way. First, because all data is gathered similarly, institutions can evaluate the comparable data through auditing. Audits allow institutions to assess

processes and outcomes, and for the police they become a form of discipline[71] to ensure that officers are "correctly" completing the cases by acquiring all the institutionally-defined required information. Further, this belief in the correct way of doing things leads to uniformity, and the uniformity reciprocally creates the idea of *closure* and *certainty*. Because all reports are to be completed in the same way, then there are set parameters of what steps are required to resolve problems. As Ericson and Haggerty (1997) state, the parameters give officers the ability to "decide whether something should be subject to policework" (p. 383), and once these prescribed steps are completed and parameters are met, the case is closed. The report now meets institutional requirements. This provides closure and certainty. The case is closed when all requirements have been met, and one can be certain that the case is closed correctly when the criteria has been met.

For the BI, as shown above, there are two basic forms which are used to gather information (the SF-86 and SF-85). These forms gather the same information from all the individuals that are going through the security clearance process. The forms set boundaries on the information that needs to be gathered and allow for oversight from government in order to compare the results of the reports. The SF-86 fits right into the idea of closure and certainty in its first line. The form reads, "All questions on this form need to be answered completely and truthfully in order that the Government may make the determinations described below [eligibility of a national security position] on a complete record" (USOPM, "Questionnaire for National Security Positions," n.d., p. 1). The form then, defines the scope of the BI and allows for the "complete" investigation and eventual determination of the clearance. When the form is completed, an individual's life is represented on the paperwork, and this allows the individual to be "thoroughly" and "appropriately" investigated in order to determine the "whole person."

The SF-85P also identifies the role the form plays and also sets the parameters for any other information gathered. This form states, "In addition to the questions on this form, inquiry

[71] According to Ericson and Haggerty (1997), Foucault's (1978) idea of discipline involves "the techniques and practices by which the human body is made subject to regular and predictable routines" (p. 91).

also is made about a person's adherence to security requirements, honesty and integrity, vulnerability to exploitation or coercion, falsification, misrepresentation, and any other behavior, activities, or associations that tend to show the person is not reliable, trustworthy, or loyal" (USOPM, "Questionnaire for Public Trust Positions," n.d., p. 1). This message establishes the importance of the form and also describes the extent of additional fieldwork that might be completed by the investigator. The statement gives the appearance that there is a set way to do things and once these things are accomplished, the case is closed with certainty of its merit.

Implications

Uniformity

The implications from the scientized way the form gathers information causes two issues for the BI. First, the standardization which allows for audits may appear to be positive on the surface. The conclusions drawn from chapter four even reflect that a call for standardization for oversight of the BI process was one of the overwhelming results of the Congressional discussions about the BI. For instance, Senator Ron Johnson stated, "If we could apply these standardized type of processes across the government, I think we would be in a far better place" (*Safeguarding Our Nation's Secrets: Examining the Security Clearance Process*, 2013, p. 5). There are drawbacks to having uniform, standardized procedures however that emerge upon a closer look at the form, especially for the BI form which is not receiving thorough Congressional attention. By allowing uniformity, the form sets up a process of box-checking which may fail to encourage additional work outside the framework of the requirements.

To elaborate on this box-checking, according to Ericson and Haggerty (1997), with the scientization of policework, "police officers inevitably must think and act according to the concrete and discrete terms of the formats within which they communicate" (p. 383), and "[t]he form is *the* prospective means towards working towards certainty and closure, providing the basis for action and at the same time accounting for the action taken" (p 384). Further, "[e]ffecting closure and certainty becomes simply a matter of completing whatever administrate knowledge requirement is demanded by the communication format" (pp. 384-5). Thus, when forms are scientized in a uniform way, the form then essentially facilitates box-checking: as long as a set of steps were

conducted as based of the risks the form identified, then the issue is supposedly legitimized for closure and certainty. If an audit were to ensue, then the matter would reflect as being complete since all boxes were checked.

Box checking is a problem for the BI, and this was even pointed out by Senator Claire McCaskill. While McCaskill wasn't specifically talking about the *applications* step (so these statements don't appear in the appendix's "Application" research data section and instead the "Investigative" section), her comments have direct implications on the application process. McCaskill condemned the investigations process and concluded that the BI has just become a process of checking boxes. An investigator is required to meet the minimum requirements of OPM, and nothing else is needed for a case to be considered complete by adjudications if the information gathered meets the institutional standards. These standards can be problematic though, and McCaskill illustrated this position when she confronted OPM's General Counsel. She spoke her concerns that the BI process as a way to guarantee individuals are vetted is beholden to the limitations of a standardized process and said, "But the notion that you are calling what you are doing quality control, Ms. Kaplan, is probably, I think, offensive, because I think there is just a lot of checking boxes going on. Was this report obtained? Yes." (*The Navy Yard Tragedy*, 2013, p. 33).

What McCaskill was referring to was an example from Alexis' BI. Upon examination of his file after his murders, there was no police report entered in Alexis' adjudicative file about an incident involving Alexis and the Seattle PD in 2004. One reason given for this lack of report was that the Seattle PD did not cooperate with OPM to provide this document, but an even more interesting matter is that there was no requirement to obtain a police report of this document (*The Navy Yard Tragedy*, 2013); only a court disposition was needed that provided the minimum amount of facts about the case (H. Rep., 2014). So in fact, the investigator did meet requirements for Alexis' case (*DC Navy Yard Shooting*, 2014) despite that the police report containing information about Alexis' shooting out a stranger's tires (which subsequently may have cost him his clearance, which gave him access to the Navy Yard) was not provided. Sterling Phillips, the Chief Executive Officer of USIS (who conducted this investigation) reaffirmed that requirements

were met and stated, “Our performance goals for all cases, including Snowden or Alexis, are to strictly follow the OPM process and to meet all OPM standards for quality in our work. If we ever fail to do so, we are promptly notified by OPM with a detailed description of any defects. All indications to USIS are that we met all standards on each of these cases” (*DC Navy Yard Shooting,* 2014, p. 42). In the case of Alexis then, all requirements were met. Investigators were doing their jobs. So while on the surface it seems that the omission of this record was an anomaly, in reality, the record was never required.

I would go further to suggest that not only was the record not required, I would suggest that there was more incentive not to acquire this record. According to news reports, investigators have nearly impossible timeliness metrics to meet (Davenport, 2015; Kyzer, 2015), and at least in the case of Alexis, if it had even been possible to obtain Alexis’ record (again, depending on Seattle PD’s cooperation), any delay from Seattle PD would have delayed the case overall.[72] This would have reflected poorly on the investigator, so while it may have been possible to obtain a report after debating with the Seattle PD, one could argue that there is more incentive to complete the case without a police report rather than obtain a report that is not required to be obtained.[73]

McCaskill illustrates why this box-checking is a concern when she talks about her experience as a prosecutor and issues of mental illness. In the context of Alexis’ struggle with mental illness of which he suffered when he thought he heard voices, McCaskill states:

> I am a former prosecutor, and the vast majority of cases that would reveal a mental disturbance will not have a disposition. The criminal justice system does a very bad job of adjudicating the mentally ill because with the mentally ill really, from a prosecutor’s standpoint, if they have not hurt anyone, putting them in prison sometimes creates more problems than it solves. So most prosecutors, when they are confronted with a mental illness issue, like someone who says they have heard voices, someone where the police have been called to a motel room on a disturbance where someone says there are microwaves coming through the vents and, ‘People are here to get me,’ they will do a police report, and most of the time the police department will not even try to file charges.

[72] Additionally, cases automatically close after forty days, even if the case is incomplete (*Safeguarding our Nation’s Secrets: Examining the Security Clearance Process*, 2013).

[73] This also does not mean malicious intent on the investigator’s part either. If an adjudicator only needs a court disposition for evidence of criminal activity (and not a police report), I would suggest this implies that the action isn’t really important, it is a matter of whether or not the individual was convicted of a crime that is an issue.

> That is a disturbance call that is related to someone that, in their minds, they do this all the time. (*The Navy Yard Tragedy*, 2013, p. 32)

This statement illustrates that if only a court disposition is required, information that never gets to the courts may be overlooked, and a requirement to obtain only a court report leaves the investigation lacking in significant information that an individual may have a condition that the government considers a risk. It could appear then that checking boxes becomes the goal rather than a gathering of explanatory information.[74] Further, without a critical look into what procedures were standardized (or how times have changed since the standardizations), inadequate processes may be set in place which continue to be replicated on a wide scale since the processes are supposed to be the same for all investigations.

Box-checking and the subsequent replication of inadequate information due to a lack of attention can also be illustrated by the application form too, and the dangers can be seen in two ways. Not only does the replication of inadequate processes pose risks to national security, the replication can also cause risks to the personnel involved in these processes. I describe both of these problems in the following ways.

First, for national security implications, the form overwhelmingly lacks attention on the Internet and computer activities. Neither the SF-86 or SF-85 form format really addresses the Internet beyond that the SF-86 requires the subject of investigation to list an email. Also, there are only three questions on the SF-86 at the end of the questionnaire near the questions about terrorism[75] that address the misuse of information-technology systems (USOPM, "Questionnaire

---

[74] While McCaskill's words may be more suited to addressing the adjudications step because it deals with how adjudications determines what information is needed for the determination of a clearance, the example still illustrates the point that standardized procedures can cause problems because investigations and adjudications are based on the application's foundation. As an aside, an additional point to note is that adjudications was surprisingly the second least discussed step but is not addressed in this study due to the scope of the project. Adjudications, like the applications, sets a foundational basis for socially sorting individuals based on information gathered by surveillance.

[75] I note the placement of these questions because after reading the form, by the time one gets to this portion of the form, the questions are less about lifestyle and seem more about formalities to make sure the government could say they asked about this matter if anything were to come up or to be paired with a polygraph at a later date. For instance, if one was a terrorist trying to infiltrate the government in order to obtain secrets, I am doubtful they would truthfully answer the question

for National Security Positions," n.d.; USOPM "Questionnaire for Public Trust Positions," n.d.). This is in addition to the restriction that investigators are prohibited from using the Internet (H. Rep., 2014) (which is another matter not discussed further due to scope constraints).

Examples show though that it may be useful to know something about someone's online presence. For instance, Bradly Manning had listed some questionable comments on his Facebook page that may have made some officials leery about his behavior (Young, 2015). Had the form asked for information about Manning's Internet use (or policies allowed investigators to use the Internet), then additional information about Manning could have been identified. As seen through this example then, the form continues to miss key information that may help indicate problematic behavior or malicious intent by failing to ask for this information on the form.

Further, there are other examples of possible oversights on the BI form. Former State Department special agent Scott Stewart (2013) commented:

> The investigations are also only looking for very specific behaviors in the subject's past, such as criminal behavior, debt, mental health issues or drug use. These things are merely outward indicators, not real insights into the subject. Besides, a lack of these indicators does not necessarily mean that the subject will not compromise national security in the future, especially if the person is motivated toward espionage or a massive public disclosure of classified information by ideology or ego. Even many of the people motivated by money have done so more out of greed than by any demonstrable history of financial problems.

In these respects, then, the questions the forms are asking may not even be relevant to ask, and more insightful questions might be needed. As all BIs are standardized in a similar way, again the magnitude of possibly missed information is spread across a large scale.[76]

In addition to national security concerns that result from ignoring both the applications and adjudications steps, there are also social justice implications. Not paying attention to the criteria of acceptability for the BI is problematic because not only does overlooking the procedures possibly cause more national security risk through the *absence* of information gathered (such as Internet use), the overlooking of the procedures of both the form and

---

"Have you EVER knowingly engaged in any acts of terrorism?" (USOPM, "Questionnaire for National Security Positions," n.d).

[76] For ethical considerations on the use of social media and Internet information in BI's, see Young, 2015.

adjudications possibly causes social justice issues due to the information that the forms are *still gathering* (such as some types of mental health counseling and debts) and the criteria adjudications is still using to decide what is a risk.

Due to the socially constructed nature of risks, ignoring the applications step also ignores critical interrogation into the way the government defines risk. The constructed risks BIs identify (such as credit problems or tax debt) don't necessarily exist in a capital "T" truth type of way. Risks are what institutions define are risks, and failure to address the constructed nature of what is considered a risk by the BI can result in problematic conclusions. For instance, should an adjudicator consider financial issues and at what threshold? As addressed in the last chapter, what about one's ideological value of money? Should this be a consideration of the form too since one's attitude towards money also accounts for the reason people spy (Gelles, 2001)? Should adjudications consider that an individual has foreign associations? Should they consider receiving mental health treatment as an issue? Not paying attention to the criteria of risk can lead to sustained, misguided ideas about risks. Attention to the criteria used by the BI forms and application is necessary then and should not be overlooked.

To illustrate, as previously discussed in chapter four, David A. Borer of the American Federation of Government Employees stated, "The implication that financial hardship equates to disloyalty, even for employees with no access to classified information, is unsupported and offensive" (*Safeguarding Our Nation's Secrets: Examining the National Security Workforce*, 2013, p. 10). This comment was followed up further with the statement, "In fact, AFGE has found that the practice of penalizing employees based on their credit scores has had a disproportionate impact on employees, over 40 female employees, and employees of color." By stating this, Borer highlighted the dangers in overlooking adjudications criteria. Some groups are disproportionally affected by the ideals embedded in the criterion of, for instance, credit reports. It is assumed that credit problems equate to risks, and poor credit is enough justification for a clearance denial. And what about those that are not in need of money but commit actions contrary to their clearance anyway? For instance, high profile spy Alrich Ames' wife reportedly stated she didn't think Ames sold secrets for the money; rather, he was arrogant and wanted people to know he was better

than them (NOAA, 2001). Other factors seem to be at work. According to Gelles (2001), “To say that it is greed, that people spy for money, is too simplistic and doesn’t help us identify who is at risk. Most of us either need or want more money.” Too, Snowden also didn’t provide information for monetary gain.

Overwhelmingly then, while it might be useful to examine one’s financial situation, more attention needs to be spent on this area as well as other possible areas of inquiry. The criteria of what is an issue may benefit from more attention so that this social justice issue may be addressed. It would be worth looking at the correlation between finances and national security breaches. The same conditions that used to be a concern may no longer be (or have ever been) equated to disloyalty. Borer further puts this credit issue in context when he states, “Thanks to a 3-year pay freeze, sequestration in which over half of the Federal employees lost 30 percent of their take-home pay for 6 weeks, and a 16-day furlough with the shutdown, many were left unsure of how or when they would be able to pay their bills” (*Safeguarding Our Nation’s Secrets: Examining the National Security Workforce*, 2013, p. 10).

Given the recession, foreclosure crisis, and stagnating wages, the use of the credit information for the determination of a level of threat seems at least open to be debated, especially when statistics show a disproportionate impact on certain groups. Even though as discussed in chapter four the Center for Development of Security Clearance Excellence (2012) alluded to nine mitigating issue factors such as the nature, extent, and seriousness of problems, it appears credit issues are still causing denial of access, even though identifying credit problems does not *prevent* someone from selling information to pay off their debts or even being the kind of person susceptible to bribery in the first place. Further, Stewart (2013) and Gelles (2001) commented that even if financial reasons were cited in an individual’s reasons for disclosing information, often the financial reason is greed or other reasons and not money troubles.

Another example of problems with a form not receiving attention can be seen in the example of homosexuality before 2011. Before Obama did away with the “Don’t ask, Don’t tell” (DADT) policy in September of that year, the military barred openly homosexual individuals but operated under the condition that if one didn’t disclose that information, no one would ask. In

2004 however, Massachusetts legalized same-sex marriage. The SF-86 requires that the applicant list their spouse on the form to include the spouse's name, other names used, date of birth, place of birth, place of marriage, social security number, current address, phone number, and email address (USOPM, "Questionnaire for National Security Positions," n.d). An individual in this case would thus be required to list the spouse on the form, regardless of the DADT policy. This would be problematic because homosexuality in the military was banned. Additionally, according to Henderson (2010c), adjudication criteria at least in 2010 treated homosexuality as an issue, much like other sexual behaviors of "sodomy, promiscuity, adultery, group sex, cyber-sex, swinging, pornography, sadism, masochism, fetishism, bondage and degradation, homosexuality, bisexuality, transsexualism, and transvestism." While the adjudications criteria may have changed after the end of DADT (although this is not known due to a lack of published information), including homosexuality (open to debate, as well as other items on this list) as an issue is disconcerting. While this matter may not be as relevant since 2011 when DADT was repealed, it does illustrate the importance of updating the paperwork to be more sensitive of the current ideological and legal climate.

Both of these issues, financial status and sexual identity, show that when society and times change, the factors that were once declared risks no longer seem to be as risky, revealing the socially constructed nature of the criteria underlying the BI. In the context of the great recession where at its peak, 2.14 million homes were in foreclosure (Veiga, 2015), or when individuals such as Brigadier General Tammy S. Smith ("the first openly gay officer of flag rank in the United States military") are allowed to serve openly in the military (Wald, 2012), some of these old vestiges of a bygone era may seem inappropriate or offensive. Even the process of the BI overall was created in 1953 through Executive Order 10450 because Eisenhower was concerned about communists in the government. According to the Defense Personnel Security Research Center (2005), "Although not explicitly stated, the implicit goal of Executive Order 10450[77] was to prevent Communist agents from entering government service" (p. 7).

[77] Executive Order 10450 is the foundational executive order for clearances outlining security requirements for employment.

It is of note that at least one question has recently changed on the SF-86. According to *The Navy Yard Tragedy* (2013), in 2008 the SF-86 question about mental health treatment changed to allow those seeking treatment for combat-related issues to not have to list that they were seeking mental health treatment because it was thought many were not seeking treatment for combat-related issues because they knew that they would have to list this on the form. The DPSRC (2015), brings out this could also be affecting getting help for sexual assault. While the combat-related changes is a positive move, I am left wondering if there are other outdated assumptions that need to be examined.

So, overall then, if little attention is directed towards looking at the criteria used to standardize adjudications, then ultimately there may be national security and social justice implications. Although as stated, there was a discussion of making standardization a priority for adjudications and even Prioletti stated his team was looking into the matter, there was a lack of congressional discussion overall of how to fix it rather than blanket recommendations to standardize the process. In Alexis' case, because established criteria didn't require information about the arrest beyond the bare bones such as the "data/place of the offense, statement of the actual charge, circumstances of the offense, and its disposition" (H. Rep., 2014, p. 43), then no information about his charge was obtained.

In the larger context of this study, these examples show that by requiring uniformity, the form sets up a process of box-checking which may fail to encourage additional work outside the framework of the requirements. Coupled with the lack of attention on what gets standardized in this box-checking process, this example shows that there may be national security and social justice consequences. Broken processes may continue to be repeated enough times in a big enough scope so that problems such as Snowden or Alexis may occur.

Closure and Certainty

The implications from the scientized way the form gathers information causes a second problem for the BI due to its effects of *closure* and *certainty*. As Ericson and Haggerty (1997) discussed:

> Scientization within established communication formats has the intended consequence of effecting closure and certainty in police work. It allows the police officer to prospectively decide whether something should be subject to police work (whether it fits and established form), and if so, to complete the task in concrete and discrete risk management terms. (383)

So with standardized procedures comes the idea that there is a right way to conduct an investigation, and once these things are accomplished, the case is closed with certainty of its merit. Because there is a concrete way to do things, when those things are completed, then there is closure.

A belief in the thoroughness and appropriateness of completing a predetermined sequence of activities begins with the rhetorical space carved out by the application process and form. As discussed, the form constrains and moderates the investigative activity that needs to be accomplished. The idea that Snowden and Alexis somehow "slipped through the cracks" exemplifies this belief in the process. If the two were to have supposedly "slipped through the cracks," then there must have been some procedure that had failed (Young, forthcoming). The BI procedure which had certainly produced a closed case must have been botched in some way (and thus provides the exigence for the congressional hearings about the BI process).

The certainty and closure that sets the BI on perhaps an unreliable pedestal is the second consequence of the scientization of this process. It is assumed that if all procedures were followed, then there is closure and certainty; however, there just may not be an airtight system in the first place. While it is true that the BI may identity probabilities of risk, it shouldn't be a surprise that Snowden or Alexis did something contrary to the values that the BI is supposed to uphold. The BI identifies probabilities based on past behavior; it does not guarantee the future can be predicted with certainty. The language of "slipping through the cracks" then isn't a phrase that should make sense for the context of the BI; this phrase implies that there is an airtight system where one "slips" through (Young, forthcoming).

A skeptical stance towards BIs is not a stance people usually take though. As discussed in chapter one, in many contexts, contemporary society tends to use BIs as a safety mechanism for preventing some type of undesirable event. Whether it be for screening refugees, determining the suitability to own a gun, evaluating whether someone is a competent renter, or making the

determination if someone should have access to federal facilities and classified information, BIs are often used as the way to eliminate risk. For instance, the full title of the Brady Act which requires background investigations before acquiring a handgun is the "Brady Handgun Violence Prevention Act" which explicitly contains the word *prevention* (H.R. 1025, 1993). While the success of this bill is not being examined, the idea that it is preventative is important. The title supports the idea that a background check will prevent the wrong people obtaining a handgun. Similarly, after the November 2015 Paris attacks, the language of the SAFE Act proclaims that the BI will provide certification that an alien trying to enter the US is not a threat (H.R. 4038, 2015), and the discourse surrounding BIs for landlords affirms that criminal checks will provide community safety, prevent criminal applicants, and determine qualification of appropriate renters ("Tenant Screening," n.d.).

Overall, a collective belief in the BI illustrates Burke's theory of identification. At the beginning of this dissertation, I talked about identification in relation to the idea that words are symbols, and people seek to have agreement on the meaning of terms though *identification.*[78] Burke (1969) stated, "You persuade a man only insofar as you can talk his language by speech, gesture, tonality, order, image, attitude, idea, identifying your ways with his" (p. 55). We identify things to make sense of the world. While I used this idea at the beginning of the dissertation to ground the study's method of looking at the congressional documents in two different ways, it is also useful to see identification in respects to BIs overall. There is a shared dependency on the BI as a way to prevent and eliminate risks, and the BI often goes unmarked as a terministic construction that spans discourse communities.

To be fair, there were some voices throughout the study that did question the BI. It is interesting to note though that of the examples listed below, the entries are all from Greg Marshall, Chief Security Officer of DHS. While there are other voices such as Senator Tom

[78] Of interest is the idea that for Burke, identification means a shared understanding, but for surveillance studies, identification means the imposition of characteristics and traits from an outside source that doesn't necessitate agreement. While this idea won't be explored further here, it is an interesting point that warrants further analysis.

Coburn and General Leonard Eric Patterson (*The Navy Yard Tragedy*, 2013),[79] these were the most striking to me because of Marshall's persistence given his leadership position in DHS's security department. His objections are what first clued me into the larger assumptions that are made about BIs. Table 36 originally appeared in chapter four but is listed below to highlight some of these stances.

Table 36.

General Distrust of BIs Beyond the Federal Process.

Reason	Definition	Example
Can't eliminate risk	No matter how good BIs are, they can't eliminate all risks.	"I need to make clear, however, that security aims to manage risk, not eliminate it" (*The Insider Threat*, 2013, p. 12).
Can't find everything	BIs can't find everything regardless of trying.	"It is important to note that any background investigation, no matter how rigorous, is no guarantee that all relevant information is known, available, or has been included" (*The Insider Threat*, 2013, p. 12).
Can't predict the future	BIs aren't able to predict the future.	"Even those who have successfully undergone the most rigorous set of background checks available--even a comprehensive polygraph examination--may someday prove untrustworthy" (*The Insider Threat*, 2013, p. 14).
Only look at past	BIs really only offer a look at the past.	"Ultimately, a Federal background investigation only examines past behavior and is sometimes based on limited available Information" (*The Insider Threat*, 2013, p. 14).

Because of the predominance of the reliance on the BI, it is important to study the BI phenomena. This is a difficult task to do scholastically though because there is a lack of academic literature analyzing the BI more than just as a process. As discussed, BIs are often normalized and not interrogated as a process; there is an assumption that in order to vet someone as trustworthy, a thorough BI based on probabilities of risk will prevent future adverse events.

[79] See details in the Appendix C "Miscellaneous" document for more example texts.

Although this language often comes from public sources,[80] academic literature seems to follow the same trend. First, it is hard to even find literature studying BIs. Terpstra, Kethley, Foley, and Wanthanee noticed this first in 2000 when they stated, “Unfortunately, no empirical data has been gathered regarding the reliability or validity of background investigations” (p. 45). Additionally, as shown below, much of the discussion of this process occurred in the late-1990s and early 2000s. Regarding what does exist, a large chunk of information published on BIs and related topics is often dated and comes out of criminology and law enforcement (Beckman, Lum, Wyckoff, & Wall, 2003; Bradford, 1998; Decicco, 2000; Kitaeff, 2011; Ritch, 1997; Snowden & Fuss, 2000; Wilson, Dalton, & Scheer, 2010; Wright, 1991), business (Doty-Navarro & Kleiner, 2000; Ferraro & Spain, 2006; Oldham, 2011; Woska, 2007), or law (O'Brien, 2010; Terpstra, Kethley, Foley, & Wanthanee, 2000). Most of these sources don’t stray from procedural techniques and best practices or ways to prevent litigation. For instance, Ritch (1997) takes the procedural stance has the disclaimer, “**This is not a manual about theory!**” (1997, p. 7) (emphasis in original) reminding his audience he is not addressing underlying assumptions of the BI. Also, Woska (2007) writes about avoiding litigation and discusses that employers are often caught in a conundrum as to whether they check backgrounds at the risk of lawsuits based on character defamation or don't conduct checks and risk lawsuits for a negligent hiring process. Both though avoid questioning the overall discourse surrounding the role of the BI.

Of the literature that does question practices common in the BI such as criminal background and credit report checks, the majority comes from business journals and falls under the related term of “pre-employment screening” rather than BIs. This term seems to draw more criticism than the term BIs and has more sources that complicate the idea of gathering information for the purpose of prediction. Pre-employment screening literature tackles topics such as the prediction of on-the-job violence (Slora, Joy, Jones, & Terris, 1991), use of credit reports when screening for future employees (McDaniel, Lees, & Wynn, 1995), use of social media for pre-employment (Stoughton, Thompson, & Meade, 2015), the use of employment interviews for

[80] Note the discourse from Donald Trump when he calls for “extreme vetting” (BBC, 2016) to ensure safety or the vetting of Syrian refugees (Altman, 2015).

future performance (McDaniel, Whetzel, Schmidt, & Maurer, 1994), and the use of pre-employment screening for security risk (Schuessler & Hite, 2014).[81]

As McCrie (2007) shows though when he states pre-employment screening incorporates background investigations, there is a difference between the two concepts. This difference is hard to see however, and oftentimes the two words seem interchangeable. For instance, a criminal record check is sometimes considered part of pre-employment screening (Davies & Hertig, 2008), and other times like in the case of a federal investigation, it is considered as part of a background investigation and the terms "pre-employment screening" are not used (e.g., *DC Navy Yard Shooting*, 2014). Davies & Hertig (2008) even use the term "preemployment background checks" (p. 375). For the purpose of this dissertation though, I will make a distinction based on two definitions. According to McCrie (2007), pre-employment checks are done to determine whether perspective personnel are "trustworthy and capable" (p. 363). On the other hand, according to Ferraro and Spain (2006), background checks are used to "(a) verify the accuracy and completeness of statements made by the candidate, and (b) develop additional relevant information concerning the candidate necessary to make the informed decision" (pp. 436-7). While one could argue that the two definitions could mean similar things, I emphasize the verification of information as given by an employee and the development of additional information as what distinguishes a BI from a pre-employment screening. The BI is there to validate the responses provided during pre-employment screening, and also there to develop additional details if issues are found to be present. Overall then, while there is some literature

[81] Also of note, several of the articles are coauthored by the same individual, Michael A. McDaniel who, according to his CV, formerly worked at OPM as a Personnel Research Psychologist, at Booz, Allen & Hamilton, Inc. as an Associate (Management Consultant), and worked at the Defense Personnel Security Research and Education Center as a Personnel Research Psychologist, all of which are agencies discussed in this dissertation (McDaniel, 2016). More specifically, OPM conducts the BIs, Snowden also worked for the contractor Booz Allen Hamilton (after McDaniel's listed tenure in the late 1980s/early 1990s), and the Defense Personnel Security Research and Education Center has conducted several studies about BIs as evidenced by the already discussed Lang article and the to be discussed articles by Ralph M. Carney and Lisa A. Kramer, Kent S. Crawford, Richards J. Heuer, Jr., & Robert R. Hagen. This further reduces the breadth of those writing about the subject since many of the sources come from the same areas.

problematizing some aspects of the elements that can constitute a BI, a more direct analysis on the fundamental principles of specifically the BI in particular is lacking.

To be thorough, there are some articles that do address issues of the BI specifically (Appel, 2014; Rogers, Boals, & Drogin, 2011; McDaniel, 1989), but these still too are limited. There is still a lack of literature theoretically critiquing the BI overall. Topics in this section discuss again more specific pieces of the BI such as advocating the use of Internet for BIs (Appel, 2014), adding psychological testing to BIs to detect deception (Rogers, Boals, & Drogin, 2011), and adapting BIs to incorporate more than self-disclosed information (McDaniel, 1989).

Additionally, there are critiques about the BI coming from government sources (Defense Personnel Security Research Center 1996; Defense Personnel Security Research Center, 2001; Moynihan, 1997). These authors question the importance of sources in investigations (Defense Personnel Security Research Center, 1996; Defense Personnel Security Research Center, 2001) or the investigation and adjudications criteria (Moynihan, 1997). Ultimately though, these reports are coming from a limited source and address more particular elements of the BI rather than interrogate the overall normalization of the BI as a way to prevent inappropriate behavior.

Overall, this study and this whole conversation raises fundamental questions of the use of the BI. Although there are some voices that bring up the fallibility of the BI, discourses often identify BIs as if they were *the* mechanism that will prevent future endangerment.

In conversation with the first point, with lack of attention to the processes, BIs may have just become routinized procedures or rituals which aren't calibrated to provide necessary information. Instead, they are more or less designed to have investigators report in a standardized way for the purpose of fact-checking and not really to gather a breadth of information about an individual or something that may better represent a "whole person." The BI has become what Staples (2000) refers to as a "meticulous ritual of power" whereby it is a knowledge-gathering activity using techniques "faithfully repeated" and "often quickly accepted and routinely practiced with little question" which are "intended to discipline people into acting in ways" that others have deemed appropriate (p. 3). While Staples was referring more to the technology's partnership with surveillance, his point is still applicable. Coupled with Ericson and

Haggerty's (1997) research, BIs urge and constrain BI investigators to write in certain ways and gather certain information to complete these BIs as defined by law, whether or not those that create the law have really examined the processes that it outlined to be carried out. The BI becomes just a technique repeated over and over rather than a conscious attempt to obtain a representative picture.

Additional Uses for this Research

While this study has implications for rhetoric and BIs, it also has implications for other fields of research to include rhetoric and composition, and professional/technical writing.

The Study Overall

The first implication comes from a look at the study *overall* (and not a specific point due to conclusions of the study), and there are several points under this heading. First, the method is useful. Not only was I able to use qualitative content analysis to accomplish rhetorical analysis, I was also able to incorporate surveillance studies as a terministic screen in order to view that analysis through a frame of surveillance. This allowed me to both see what was being said while at the same time recognizing this space as place of surveillance. Even though the documents never referred to the BI as surveillance,[82] by using surveillance studies as my terministic screen, I drew the connection between the BI and surveillance. This same screen could be used in the rhetoric, composition, or professional/technical communication classroom in order to identify other spaces of surveillance. For instance, pedagogically, students could identify places in their lives where surveillance is present and analyze the effects of monitoring. One could also look at how surveillance effects tenue, how surveillance effects the writer, or how surveillance is sanctioned by other professional documents or technical outputs.

[82] The link of surveillance to BIs was especially interesting because surveillance was not a term adopted in the congressional discourse. While one may assume a study about government investigation would mention surveillance, in all the documents I looked at, the actual word "surveillance" was only used eighteen total times, and none of the references attributed the BI to surveillance. The references were about Edward Snowden's work with *surveillance* programs, surveillance needed on programs for *government transparency*, or *specific jobs* involving surveillance such as screeners or other government agents.

Second, the study brings up that there are places of surveillance in multiple locations. Surveillance is not limited to CCTV cameras on the street operated by a law enforcement agency as a Google image search may lead an audience to believe. Surveillance can be social media. Surveillance can be supermarket loyalty cards. Surveillance can be the classroom. Surveillance is, as Lyon (2001) said, “any collection and processing of personal data, whether identifiable or not, for the purposes of influencing or managing those whose data has been garnered” (p. 2).

Schools in particular have been studies as sites of surveillance. Foucault (1977) brought out the connection in *Discipline and Punish* when he argued that schools are disciplinary institutions that fit the framework of the Panopticon and allow the observation of students for the purposes of control. Further, Gilliom and Monahan (2013) assert, “[S]chools are so completely defined by surveillance that sometimes it’s hard to even recognize it for what it is” (p. 73). For Gilliom and Monahan, registration is surveillance, medical exams, required vaccinations, attendance, hall passes tests, and grades are all surveillance. Too, schools are also testing grounds where technology such as CCTV cameras and radio-frequency identification (RFID) cards, and sites where public and private security operates to control students.

For an English classroom, a professor monitors student work by grading papers and ensuring students post to discussion boards (functioning as a surveiller that observers a student’s actions with constancy in a classroom), records a variety of grades based off student work and other factors like participation (creating a surveillant assemblage) in order to assess and monitor students (social sorting) using technology to keep track of the student (such as a learning management tool or Safe Assign). The teacher may perhaps assess risk based on student performance to predict the students that will need more assistance. In the class, students grapple with their identities as writers, and we as teachers, impose identification on the students based on our interpretations of their work.

Third, one can incorporate critical inquiring using themes associated with surveillance studies into rhetoric, composition, or professional/technical communication research. As shown in my dissertation, the issues of sorting, risk, identity, and prediction are rife with, among many issues, the concerns of race, class, and gender. For instance, my study showed the use of credit

reports' "disproportionate impact on employees, over 40 female employees, and employees of color" (*Safeguarding Our Nation's Secrets: Examining the National Security Workforce*, 2013, p. 10).

Further, there are other prevalent themes in studies of surveillance. For instance, surveillance involves 1) questions of identity. For instance, who defines the identity of those under surveillance, the watcher or the watched? 2) Surveillance also involves agency: who are the surveillers and who are the suveilled? Also, who is able resist? 3) It involves visibility and transparency: are we aware of the times we are being watched? What are the consequences of constant monitoring? Should we know if we are being watched? 4) It involves themes of interest to feminist rhetoric: are certain groups under more scrutiny such as the credit issues of non-Caucasian women over forty? 5) Surveillance involves materiality: what are the tangible aspects of surveillance? Algorithms? CCTV cameras? What are the limitations of technology as a solution? And 6) it involves discussions of literacy: do people know how to resist? Are they aware of whistleblower protections? Have some whistleblower protections been removed? These themes could be used by researchers to engage in analysis of texts in order to complete critical research which, as Blyer (1999) suggested, involves looking at "existing social structures and practice, with the aim of uncovering the workings of domination and power and thus fostering critique and social change" (p. 77). Surveillance, as shown above, allows for those connections to be explored.

Additionally, surveillance can also provide a lens for examining the act of writing. As Dobrin (1999) and Dobrin and Weisser (2002) suggested, composition research has shifted from studying the writing process "to the larger forces that affect that writer and of which that writer is a part" (Dobrin, 1999, p. 132). As shown by Neil M. Richards in his theory of intellectual privacy, surveillance is a force that very much affects the writer. According to Richards (2008), intellectual privacy as "the ability, whether protected by law or social circumstances, to develop ideas and beliefs away from the unwanted gaze or interference of others" (p. 389). Richards theorized that it is important to be able to write without the gaze of others, otherwise, we become certain subjects and our writing will be affected. Richards continued, "Surveillance or interference can warp the

integrity of our freedom of thought and can skew the way we think, with clear repercussions for the content of our subsequent speech or writing. The ability to freely make up our minds and to develop new ideas thus depends upon a substantial measure of intellectual privacy" (p. 389) For Richards, being able to think without being watched by others was very important to intellectual creation.

Although Richards (2013) was specifically speaking about government surveillance (he states intellectual privacy is our ability "to think without state oversight or interference" (p. 1935), at its core, the discussion at least has implications for the composition classroom. As discussed above, Richards stressed was that surveillance skews the way we think and effects the contents of what we produce. More specifically, Richards asserted that we are able to think, read, and communicate with others without being watched, we tend to be more creative. When we know we are being watched, however, Richards (2013) stated, "[I]t can cause people not to experiment with new, controversial, or deviant ideas" (p. 1935).

For composition studies, the idea of a surveillant presence in a classroom is an area to be explored. Further study could go into researching the impact of being watched on the writer through the lens of surveillance studies. Some research has already gone into this in social media spaces (boyd & Ellison, 2008; Donath & boyd, 2004; Marwick, 2012; Young, 2015), but it also has implications in the composition classroom. Also, Richards stated, "In order to speak, it is necessary to have something to say, and the development of ideas and beliefs often takes place best in solitary contemplation or collaboration with a few trusted confidants" (2008, p. 389). This further opens up a call for research into the definition of "solitary contemplation" or "trusted confidants. Composition research could address whether there is a possibility of "solitary" contemplation or assess whether there is a level of threshold for trust affecting someone's ability to write. Would a teacher become a trusted confidant, or is a teacher viewed as the surveillant power? All of these questions would help explore composition's effort to examine "the larger forces that affect that writer and of which that writer is a part" (Dobrin, 1999). Additional questions to consider are, do students come with varying conceptions of the role of the teacher and the way in which students are monitored? Does an international student have a different

perspective? What is the role that social media should play in pedagogy? For instance, what are the ethical limitations of requiring students to engage in social media during a class with a prospective public audience especially with this dissertation's discussion of technological monitoring and big data in mind? How does a public audience change in collaborative situations, and how does a student's writing or research change knowing that someone is watching them? We may strive to find an authentic audience for our students, but with that come implications of surveillance. Also, is there a difference in writing if a public audience for social networking[83] in which strangers or unknown individuals are the watchers verses and audience of known associates in a social network? All these questions add possibilities for future research.

The Form

The second major implication arises from a discussion of the *form* rather than just the study overall. The form is critical in transmitting surveillance, and it becomes a technology, or tool, of knowledge creation by way of assemblage. By establishing the framework for information gathering, various entities can collect various information from a variety of sources. Then various agencies can look at the data gathered to decide whether or not to grant a clearance. The continued use of this form without proper attention, however, is an ethical concern. This concern is best seen through a discussion of professional and technical communication.

There are many characteristics to professional and technical documents, and according to Dobrin, Keller, and Weisser (2008), the professional and technical document should be, among many characteristics, clear and correct, concise, and rhetorical. According to the authors, to be *clear and correct*, a document should "describe every aspect and provide every detail about the subject that an audience needs" by adhering to proper grammar, punctuation, usage, and style. For a document to be *concise*, the form must "work to eliminate superfluous words, phrases, and sentences" (p. 9). The authors provide the example, "Do not use your cell phone when driving" which clearly states an intention without excess verbiage. For a document to be *rhetorical*, the document should use effective language to persuade an audience, and the document's writer

[83] For the difference between social network and social network*ing*, see boyd, d., & Ellison, N. (2008).

must think rhetorically “which means considering how documents solve problems, affect an audience, and one’s credibility as a worker” (p.10).

In this sense then, the BI’s Standard Forms meet characteristics seen in business documents. First and second, for those creating the document, the document was written clearly, correctly, and concisely such as question one which stated, “Provide your full name. If you have only initials in your name, provide them and indicate "Initial only." If you do not have a middle name, indicate "No Middle Name." If you are a "Jr.," "Sr.," etc. enter this under Suffix” (USOPM Questionnaire for national security positions, n.d.). Although it appears to be a lengthy question, like the other questions on the form, it is thorough but brief. It covers the possible variations to a name within the confines of the bureaucratic structure. Although the blank form in total is one hundred twenty-seven pages, the questions are all command-type sentence such as the name example.

Third, the form is also written rhetorically in the sense that it creates a rhetorical situation by defining and constraining a space of risk, and it persuades the applicant to provide information to explain how the individual does/does not meet the risk criteria. As the directions advised, “Providing this information is voluntary. If you do not provide each item of requested information, however, we will not be able to complete your investigation, which will adversely affect your eligibility for a national security position, eligibility for access to classified information, or logical or physical access” (p. 1). Further, the form spelled out the punishment for purposely entering false information or omitting information that should be listed. In addition to advising the applicant that a clearance or access would not be granted, the form stated that “knowingly falsifying or concealing a material fact is a felony which may result in fines and/or up to five (5) years imprisonment” (p. 2). Although the form does this by using threats and fear, it does motivate its audience to action.

Another characteristic that Dobrin, Keller, and Weisser (2008) discussed that a professional and technical document should be, however, is ethical. The authors simplify ethics to mean “making right or wrong decisions” (p. 11), and for a document to be ethical, writers must make decisions that “produce, shape, and convey information to audiences that use that

information for various purposes" (p. 11). Additionally, "Writers must seek to provide information that can be used not just efficiently and successfully, but also safely."

In terms of ethics, the BI form falls short. By Congress not discussing the questions on the form or even interrogating if the adequacy of the questions, OPM and Congress fail to interrogate if they are making the right or wrong decisions for information that the form is helping produce and shape. As shown in the dissertation, this has national security and social justice consequences. Since the BI is ultimately used to sort and predict who will be granted or denied a clearance, then attention should be directed to this form.

For studies of professional and technical writing, taking this conversation more broadly, beyond just this discussion about ethics and BIs, surveillance has implications for other professional documents, especially those gathering biometric or other personal data from a variety of sources. Job applications, online shopping or social network sites, membership into Fantasy Football leagues, or almost many other scenarios that could be imagined all have forms which ask for personal information. While we could see some of these forms as types of voluntary surveillance, or as Whitaker (1999) calls a "participatory Panopticon" where people willingly give their information in exchange for certain corporate benefits, an assemblage of personal information, regardless of why or how it was gathered, at the very least if stored electronically creates a data double which continues to exist until whoever is in charge of storing the information gets rid of the data. At some point, this data may be used as a part of other assemblages too, and as Lyon (2007) brings out, the more data that is gathered, "it becomes progressively more difficult to disappear" (p. 115). Given the data breaches such as Target and Home Depot which exposed the information of millions of customers (Sidel, 2014), disappearing from visibility is an important consideration.

Those involved in information gathering then, should take notice of their practices. For surveillance workers, at the most basic level, the form should be taken into consideration so that it doesn't collect unnecessary data. Writers and creators of forms then, especially as technology begins to track more information and big data analytics continue to be able to provide more data, need to be more cognizant of what the information they help gather will be part of. In a way, this

is the conundrum that Edward Snowden faced. Although Snowden was more clandestine than overt like an Standard Form, Snowden became a part of the surveillance gathering system, and he came to a conclusion that ethically the public needed to be told about the surveillance programs he observed. While I am not advocating for Snowden's actions, he does present an example of how an individual caught in a surveillance system evaluated their role in gathering information in terms of their own ethical limitations. Other writers similarly may want to think about what is being done with the information gathered by documents they produce. Even the anonymous gathering of metadata by advertisers illustrates the possibilities of ethical considerations for which some working in the industry resist.[84]

What is needed then is a form of surveillance literacy for surveillance ethics. In a time of possibly constant surveillance due to technological capacity, professional writers, or really anyone involved in gathering information or involved in surveillance systems, should understand what will be done with the information being gathered. A meta-awareness of the possible effects of surveillance when constructing forms such as the BI (or any other workplace document) would be helpful. A meta-awareness is also relevant too, to not just to assess one's own ethical limits of gathering information; it is also useful for identifying sites of surveillance in the first place. As this dissertation showed, the word "surveillance" wasn't even used for the BI even though characteristics of surveillance are present.

This dissertation presents at least eight heuristics for surveillance literacy analysis in the form of the eight characteristics I identified in surveillance: constancy, surveillant assemblage, surveillers, social sorting, risk, prediction, identity, and technology. When creating any rhetorical space, one could run through the different categories and ask a question based on circumstances to determine if a space facilitates surveillance and determine one's subsequent ethical expectations when operating in these spaces. For instance, one can look at their space for indications of constancy. As Lyon (2007) stated, "electronic technologies increasingly permit

[84] For instance, the advertising company Unonomity asserts they strive to "to disrupt the advertising industry & take back control over our #privacy #security & #freedom" (@UnonimityUser. 2016).

constant and mobile surveillance across spheres of everyday life," and computers can now track people all the time (p. 199). With this in mind, one could ask questions such as, does this space allow for constant surveillance? How long will I be gathering information? How will I be gathering information? What are my personal ethics for this situation? For surveillant assemblage, one can determine where sources of data are coming from. For surveillers, one could determine who is gathering the information. For social sorting, one can explore questions of the purpose of the data. What will the data be used for? Are any groups disproportionally targeted? For risk, what is being determined as risk? How are those conclusions being drawn? For prediction, how is the data gathered being used for future implications? For instance, am I trying to anticipate shopping behaviors or predict where crime can occur? Am I using technology such as big data analytics for these predictions? Am I comfortable allowing technology to create a heuristic or shortcut in my personal judgement? Should I assume that because software suggests a person will be a criminal that this will actually happen?[85] For identity, am I making assumptions about who someone is with the data I've gathered? How accurate are my assumptions? And for technology, what technology am I using? Is it facilitating the other characteristics of surveillance such as constancy, social sorting, and prediction? How long will the data be stored? Overall, this was just a brief discussion of these elements, but it does stress a need for surveillance literacy and present the idea that surveillance exists in unexpected places, and attention should be paid to all spaces due to possible ethical concerns.

Conclusion

Overall, this dissertation showed the following: 1) overwhelmingly, Congress called for more standardization and oversight of the BI process in general. 2) However, the applications step of the BI was the most overlooked step of the process, and risk was the most discussed. 3) The call for uniformity but lack of attention to one major step in the process can have implications for national security and social justice matters because uniformity leads to information being

[85] See (Anguin, Larson, Mattu, & Kirchner, 2016) as an example. In this story, the authors discuss using statistics to predict future crime and an introduced reform bill suggesting prediction technology should be used in Federal cases.

gathering in a scientized way which leads to a sense of closure. This sense of closure further leads to misplaced trust in the BI as airtight vetting ritual. It is not fool proof, however, and the lack of attention to what gets standardized may lead to some important elements such as the Internet being overlooked and personal information about applicants may be unnecessarily gathered. Further, 4) spaces of surveillance exist in places not necessarily labeled as "surveillance." Surveillance can operate in many places and through means as simple as a form. This conclusion opens up a variety of ways in which surveillance can be examined in the rhetoric, composition, and technical/professional communication classroom. Surveillance can become a lens for research and a heuristic to determine one's personal ethics.

While I started this dissertation exploring the congressional discourse surrounding BIs after Snowden and Alexis, I ended up emphasizing the importance of writers' awareness of surveillance and awareness of their ethical expectations for their work. While there were many lessons learned in between, I come to the overall conclusion that consideration should be made by those involved in known, or possibly unexpected, places of surveillance. For those researching in rhetoric, composition, and professional/technical writing, this opens up a wider variety of space to think and research. By thinking through surveillance, the field can provide another layer of analysis that, as Snowden's revelations and subsequent public outcry showed, is an area that is quickly gaining in importance. From the BI and beyond, critical attention should be directed towards spaces and methods of surveillance, and as was shown by this dissertation, rhetorical inquiry provides a robust approach for this exploration.

REFERENCES

113th Cong. Rec. H.R. 2860 (daily ed. January 14, 2014) (statement of Mr. Farenthold). Retrieved from ProQuest Congressional Database.

160 Cong. Rec. H200 (daily ed. Jan. 14, 2014) (statement of Rep. Cummings). Retrieved from ProQuest Congressional Database.

Aas, K. F., Gundhus, H.O., & Lomell, H.M. (Eds). (2009). *Technologies of insecurity: The surveillance of everyday life*. New York: Routledge-Cavendish.

Adjudicative guidelines for determining eligibility for access to classified information. (2006, February 3). Retrieved from http://www.state.gov/m/ds/clearances/60321.htm

"Algorithms." (n.d.). Retrieved from https://www.google.com/insidesearch/howsearchworks/algorithms.html

Altman, A. (2015, November 17). This is how the Syrian refugee screening process works. Retrieved from http://time.com/4116619/syrian-refugees-screening-process/

Anguin, J. Larson, J. Mattu, S. & Kirchner, L. (2016, May 23). Machine bias: There's software used across the country to predict future criminals. And it's biased against blacks. Retrieved from https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing

Appel, Edward J. (2014). *Cybervetting*. CRC Press. Retrieved from http://www.myilibrary.com?ID=693883

Aristotle. (1990). *Rhetoric: Book I*. In P. Bizzell & B. Herzberg (Eds.), *The rhetorical tradition: Readings from classical times to the present* (pp. 151–60). Boston: Bedford Books of St. Martin's Press.

Barnard-Wills, D. (2009) *The articulation of identity in discourses of surveillance in the United Kingdom* (Doctoral dissertation). Retrieved from University of Nottingham http://eprints.nottingham.ac.uk/10850/1/ Identity_in_discourses_of_surveillance.pdf

Barnard-Wills, D. (2012). Surveillance and identity: Discourse, subjectivity and the state. Burlington: Ashgate.

Barnard-Wills, D. (2014). The non-consensual hallucination: The politics of online privacy. In A. Jansson and M. Christensen (Eds.), *Media, surveillance and identity* (pp. 165-182). New York: Peter Lang.

Barr, S. (2003, April 23). For once-federal background investigators, privitization leads to its own kind of check. Retrieved from https://www.washingtonpost.com/archive/local/2003/04/24/for-once-federal-background-investigators-privatization-leads-to-its-own-kind-of-check/b8cf0089-c2a7-4704-adbb-4554a4ec9e43/

Bauman, Z. & Lyon, D. (2013). *Liquid surveillance.* Cambridge: Polity Press.

BBC. (2016, August 16). Donald Trump calls for 'extreme vetting' of immigrants to US. Retrieved from http://www.bbc.com/news/election-us-2016-37086578

Beach, J.M. (2012). *Kenneth Burke: A sociology of knowledge, dramatism, ideology, and rhetoric.* Austin: West by Southwest Press.

Beck, U. (1992). *Risk society: Towards a new modernity.* London: Sage Publications, Ltd.

Beck, E. (2015). *Computer algorithms as persuasive agents: The rhetoricity of algorithmic surveillance within the built ecological network.* (Electronic Thesis or Dissertation). Retrieved from https://etd.ohiolink.edu/

Beckman, K., Lum, C., Wyckoff, L., & Wall, K. L. (2003). Trends in police research: A cross-sectional analysis of the 2000 literature. *Police Practice and Research, 4*(1), 79-96. doi:10.1080/1561426032000059204

Bennett, C., Raab, C. & Regan, P. (2003). People and place: Patterns of individual identification within intelligent transportation systems. In D. Lyon (Ed.), *Surveillance as social sorting: Privacy, risk and digital discrimination* (pp. 153-176). New York: Routledge.

Bernier, A. (2016, February 24). How Peoria police are using new technology to better predict when and where crime will happen. Retrieved from http://science.kjzz.org/content/269439/how-peoria-police-are-using-new-technology-better-predict-when-and-where-crime-will

Bizzell, P. & Herzberg, B. (Eds.). (1990). *The rhetorical tradition: Readings from classical times to the present.* Boston: Bedford Books of St. Martin's Press.

Blakesley, D. (2012). *The elements of dramatism.* New York: Longman.

Bos, W. & Tarnai, C. (1999). Content analysis in empirical social research. *International Journal of Educational Research, 31*, 659-671.

Bowker, G. C., & Star, S. L. (1999). *Sorting things out: Classification and its consequences*. Cambridge, Mass: MIT Press.

boyd, d., & Ellison, N. (2008). Social network sites: Definition, history, and scholarship. *Journal of Computer-Mediated Communication, 13*, 210-230.

Bradford, D. (1998). Police officer candidate background investigation: Law enforcement management's most effective tool for employing the most qualified candidate. *Public Personnel Management, 27*(4), 423-32.

Braun, S., Flaherty, A., Gillum, J., & Apuzo, M. (2013, June 15). PRISM is just part of a much larger, scarier government surveillance program. Retrieved September 8, 2015, from http://www.businessinsider.com/prism-is-just-the-start-of-nsa-spying-2013-6

Burke, K. (1945). *A grammar of motives.* Berkeley University of California Press.

Burke, K. (1966). *Language as symbolic action: Essays on life, literature, and method.* Berkeley: University of California Press.

Burke. K. (1969). *A rhetoric of motives*. Berkeley: University of California Press.

Burke, K. (1984). *Permanence and change: An anatomy of purpose*. (3rd Ed.). Berkeley: University of California Press.

Burke, K. (1990). *Language as symbolic action.* In P. Bizzel and B. Herzberg (Eds.), *The rhetorical tradition: Readings from classical times to the present* (pp. 1034-1041). Boston: Bedford Books of St. Martin's Press. (Original work published 1966).

Campbell, B. (2013, November 1). Ten talking points the NSA uses to justify its spying. Retrieved from http://www.pri.org/stories/2013-11-01/ten-talking-points-nsa-uses-justify-its-spying

Cassidy, J. (2013, August 20). Snowden's legacy: A public debate about online privacy. Retrieved from http://www.newyorker.com/news/john-cassidy/snowdens-legacy-a-public-debate-about-online-privacy

Center for Development of Security Excellence. (2012). Basic adjudications overview webinar. http://www.cdse.edu/documents/cdse/121912-Webinar-Transcript_LC.pdf

Clarke, R. (2013). Introduction to dataveillance and information privacy, and definitions of terms**.** Retrieved from http://www.rogerclarke.com/DV/Intro.html

Clark, C.L. (2012). *Praxis: A brief rhetoric*. 2nd Ed. El Paso: University of Texas.

Cohen, S. (1985). *Visions of social control.* Cambridge: Polity Press.

Comey, J.B. (2014, October 16). Going dark: Are technology, privacy, and public safety on a collision course? Retrieved from https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course

Congressional Research Service. (2014). The debate over selected presidential assistants and advisors: Appointment, accountability, and congressional oversight. (Report No. 40856). Retrieved from ProQuest Congressional Database.

Crow, A. (n.d.). C.V. Retrieved from http://www.angelacrow.com/wpcontent/uploads/2008/02/cv.pdf

DC Navy Yard Shooting: Fixing the Security Clearance Process. Hearing before the Committee on Oversight and Government Reform House of Representatives. 113th Cong. (2014). Retrieved from ProQuest Congressional Database.

Davenport, C. (2015, June 14). Even after Snowden, quota system on background checks may be imperiling U.S. secrets. Retrieved from https://www.washingtonpost.com/business/economy/security-clearance-contractors-still-stress-speed-over-thoroughness-workers-say/2015/06/14/00d1bd80-09fa-11e5-95fd-d580f1c5d44e_story.html?postshare=5641434489625633

Davies, S. J., Hertig, C. A. (2008). *Security supervision and management: The theory and practice of asset protection* (3rd ed.). Boston: Butterworth-Heinemann/Elsevier.

Debate over limits of government surveillance and the future of the patriot act. (2015, May 10). Retrieved from http://thedianerehmshow.org/shows/2015-05-11/debate-over-limits-of-government-surveillance-and-the-future-of-the-patriot-act

Decicco, D. A. (2000). Police officer candidate assessment and selection. *The FBI Law Enforcement Bulletin, 69*(12), 1-6.

Defense Personnel Security Research Center [DPSRC]. (1996). *SSBI source yield: An examination of sources contacted, by Ralph M. Carney.* Retrieved from http://www.dhra.mil/perserec/reports/tr96-01.pdf

Defense Personnel Security Research Center [DPSRC]. (2001). *SSBI-PR source yield: An examination of sources contacted during the SSBI-PR*, by Lisa A. Kramer, Kent S. Crawford, Richards J. Heuer, Jr., & Robert R. Hagen. Retrieved from *www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA403829*

Defense Personnel Security Research Center [DPSRC]. (2005). *Security background investigations and clearance procedures of the federal government*, by Eric L. Lang. Retrieved from http://www.dhra.mil/perserec/reports/mr05-05.pdf

Defense Personnel Security Research Center [DPSRC]. (2015). *Relevant risk approach to mental health inquiries in question 21 of the Questionnaire for National Security Positions (SF-86)*, by Jonathan Shedler and Eric L. Lang. Retrieved from http://www.dhra.mil/perserec/reports/TR_15-01_A_Relevant_Risk_Approach_to _Mental_Health_Inquiries_in_Question_21.pdf

Deleuze, G. (1992). Postscript on the societies of control. *October, 59*, 1-7.

Deleuze, G. (1995). Negotiations: 1972-1990 (M. Joughin, Tras.). New York: Columbia University Press.

Deleuze, G., & Guattari, F. (1987). *A thousand plateaus: Capitalism and schizophrenia*. Minneapolis: University of Minnesota Press.

Denzin, N.K., & Lincoln, Y.S. (2005). Introduction: The discipline and practice of qualitative research. In N.K. Denzin and Y.S. Lincoln (Eds.), *The SAGE handbook of qualitative research* (3rd ed.) (pp. 1-32). Thousand Oaks: Sage.

Dobrin, S.I. (1999). Paralogic hermeneutic theories, power and the possibility for liberating pedagogies. In T. Kent (Ed.), Post-process theory: Beyond the writing-process paradigm (pp. 132-148). Carbondale, IL: Southern Illinois University Press.

Dobrin, S.I., & Weisser, C.R. (2002). Natural discourse: Toward ecocomposition. Albany: State University of New York Press.

Dobrin, S.I., Keller, C.J., & Weisser, C.R. (2008). Technical communication in the twenty-first century. Upper Saddle River, NJ: Pearson Prentice Hall.

Donath, J., & boyd, d. (2004). Public displays of connection. *BT Technology Journal, 22*(4), 71-82.

Doty-Navarro, S.C., & Kleiner, B. H. (2000). How to effectively check references and perform background investigations of job applicants. *Management Research News, 23*(7/8), 56-62. doi:10.1108/01409170010782181

Duhigg, C. (2012). How companies learn your secrets. Retrieved from http://www.nytimes.com/ 2012/02/19/magazine/ shopping-habits.html?_r=2&hp=&pagewanted=all

Ekberg, M. (2007). The parameters of the risk society: A review and exploration. *Current Sociology 55*(3), 343-366.

Elo, S. & Kyngas, H. (2008) The qualitative content analysis process. *Journal of Advanced Nursing 62*(1), 107–115. doi: 10.1111/j.1365-2648.2007.04569.x

Enhanced Security Clearance Act of 2013 Offered by Ms. Collins, 113th Cong. Rec. S1618 (daily ed. October 3, 2013). Retrieved from ProQuest Congressional Database.

Ericson, R. V., & Haggerty, K.D. (1997). *Policing the risk society*. Toronto: U of Toronto.

Ewald, F. (1991). Insurance and risk. In G. Burchell, C. Gordon, & P. Miller (Eds.), The Foucault effect: Studies in governmentality. Chicago: University of Chicago Press.

Facility Protection: Implications of the Navy Yard Shooting on National Security. Hearing before the Subcommittee on Oversight and Management Efficiency of the Committee on Homeland Security of the United States House of Representatives. 113th Cong. (2013). Retrieved from ProQuest Congressional Database.

Federal Clearance Assistance Service. (n.d.). Federal security /suitability clearance chart. Retrieved from http://fedcas.com/wp-content/uploads/2012/05/Federal-Suitability-Security-Clearance-Chart.pdf

Ferraro, E., & Spain, N. M. (2006). *Investigations in the workplace*. Boca Raton, FL: Auerbach Publications.

Fleming, M. (2010). CCTV camera. Retrieved from https://www.flickr.com/photos/flem007_uk/4632603680/in/photolist-84niFf-pfme6U-n6mJJn-n6mszR-5hEoWd-eC3kBM-3pGkDh-nP2Bfv-8j3LGY-nwKMWi-aTJxj-8y2kky-brVVt-foWLwM-2CMQ5-c3rwyy-cgY6vs-3Jw3Bi-381SKF-6tLxp2-c1UTf-386tJq-Mh7jG-4z5BPD-knFVMs-4ow3y-6ggAP8-4ow3t-buGrc-azpGSc-pAxok-azsn43-86d4yG-Mh81m-4VWVBM-MoGeJ-8G3hVb-7degT-5rs3Bh-9zzZzy-rXVAh-8oMTmk-Mh7Eb-MhiFa-dLMo1K-cyKQtj-oaLWEs-4ovzB-3nifg-mQcvoy

Foucault, M. (1977). *Discipline and punish: The birth of the prison*. (A. Sheridan, Trans.). New York: Vintage.

Gandy, O.H., Jr. (1993). The panoptic sort: A political economy of personal information. Boulder: Westview Press.

Gates, K. A. (2011). *Our biometric future: Facial recognition technology and the culture of surveillance.* New York: New York University Press.

Gelles, M. (2001). Exploring the mind of the spy. Retrieved from http://www.wrc.noaa.gov/wrso/security_guide/mind.htm

Gilliom, J. & Monahan, T. (2013). *SuperVision: An introduction to the surveillance society*. Chicago: U of Chicago.

Gordon, N. (2011). Israel's emergence as a homeland security capital. In E. Zuriek, D. Lyon, & Y. Abu-Laban (Eds.), Surveillance and control in Israel/Palestine: Population, territory and power (pp. 153-170). New York: Routledge.

Graham, S. & Wood, D. (2003). Digitizing surveillance: Categorization, space, inequality. *Critical Social Policy 23*(2), 227-48.

Graneheim, U.H. & Lundman, B. (2004). Qualitative content analysis in nursing research: Concepts, procedures and measures to achieve trustworthiness. *Nurse Education Today, 24*, 105–112.

H.R. 490 - Security Clearance Accountability, Reform, and Enhancement Act of 2015. (2015). Retrieved from ProQuest Congressional Database.

H.R. 1025 – Brady Handgun Violence Prevention Act. (1993). Retrieved from https://www.govtrack.us/congress/bills/103/hr1025

H.R. 4022 - Security Clearance Accountability, Reform, and Enhancement Act of 2014. (2014). Retrieved from ProQuest Congressional Database.

H.R. 4038 – American Security Against Foreign Enemies Act of 2015. (2015). Retrieved from https://www.Congress.gov/114/bills/hr4038/BILLS-114hr4038ih.pdf

H.R. 5240 - Clearance and Over-Classification Reform and Reduction Act. (2014). Retrieved from ProQuest Congressional Database.

H. Rep. (2014). Committee on Oversight and Government Reform. Slipping through the cracks: How the D.C. Navy Yard shooting exposes flaws in the federal security clearance process. Retrieved from http://oversight.house.gov/wp-content/uploads/2014/02/Aaron-Alexis-Report-FINAL.pdf

Haggerty, K.D., & Ericson, R. (2000). The surveillant assemblage. *British Journal of Sociology, 51*(4), 605-622.

Hamre, J. (2013, 20 Feb.). The wrong way to conduct security clearances. Retrieved from https://www.washingtonpost.com/opinions/the-wrong-way-to-conduct-security-clearances/2013/02/20/2d0d1e2c-7554-11e2-aa12-e6cf1d31106b_story.html

Hirschfeld Davis, J. (9 July 2015). Hacking of government computers exposed 21.5 million people. Retrieved from http://www.nytimes.com/2015/07/10/us/office-of-personnel-management-hackers-got-data-of-millions.html?_r=0.

Henderson, W. (2010a). The impact of delinquent debt on security clearances. Retrieved from https://news.clearancejobs.com/2010/01/28/the-impact-of-delinquent-debt-on-security-clearances/

Henderson, W. (2010b). Security clearance: The whole person concept. Retrieved from https://news.clearancejobs.com/2010/12/27/security-clearance-the-whole-person-concept/

Henderson, W. (2010c, February 16). Sexual behavior and security clearances. Retrieved from https://news.clearancejobs.com/2010/02/16/sexual-behavior-and-security-clearances/

Henderson, W. (2015, 22 Feb.). SCARE, CORRECT and Enhanced Security Act – Security clearance legislation that died. https://news.clearancejobs.com/ 2015/02/22/scare-correct-enhanced-security-act-security-clearance-legislation-died/

Herrick, J.A. (2005). The history and theory of rhetoric: An introduction. (3rd ed.). Boston: Pearson.

Hsieh, H. & Shannon, S.E. (2005). Three approaches to qualitative content analysis. *Qualitative Health Research 15*(9), 1277-1288.

Humphreys, L. (2011). Who's watching whom? A study of interactive technology and surveillance. *Journal of Communication 61*, 575–595.

The Insider Threat to Homeland Security: Examining Our Nation's Security Clearance Process. Hearing before the Subcommittee on Counterterrorism and Intelligence of the Committee on Homeland Security House of Representatives. 113th Cong. (2013). Retrieved from ProQuest Congressional Database.

Jewkes, Y. (2004). Crime and the Surveillance Culture. In *Media & Crime: Key Approaches to Criminology* (pp. 171-198). Thousand Oaks: Sage Publications.

Kalathil, S. & Boas, T.C. *Open networks, closed regimes: The impact of the internet on authoritarian rule.* Washington, D.C.: Carnegie Endowment for International Peace.

Kelly, E. (2015a, November 19). House passes bill to block Syrian refugees, require more vetting. Retrieved from http://www.usatoday.com/story/news/2015/11/19/house-passes-bill-bar-syrian-refugees-us-without-more-vetting/76041668/

Kelly, E. (2015b, June 20). OPM hack raises questions about security of government contractors. Retrieved from http://www.usatoday.com/story/news/politics/2015/06/20/opm-hack-government-contractors/28922679/

Kim, M. (2004). Surveillance technology, privacy and social control. *International Sociology 19*(2), 193-213.

Kitaeff, J. (2011). *Handbook of police psychology*. Routledge. Retrieved from <http://www.myilibrary.com?ID=304252>

Kyzer, L. (2015, December 16). OPM update - New agency taking background investigations. Retrieved from https://news.clearancejobs.com/2015/12/16/opm-update-notifications-out-and-a-new-agency-for-background-investigations/

Lunsford, A.A., Ruszkiewicz, J.J., & Walters, K. (2013). *Everything's an argument*. (6th ed.). Boston: Bedford / St. Martin's.

Lucas, G.R., Jr. (2014). NSA management directive #424: Secrecy and privacy in the aftermath of Edward Snowden. *Ethics & International Affairs, 28*(1), 29-38. doi:10.1017/S0892679413000488

Lupton, D. (1999). *Risk.* New York: Routledge.

Lyon, D. (2001). *Surveillance society: Monitoring everyday life*. Philadelphia: Open University Press.

Lyon, D. (2003a). "Introduction." In D. Lyon (Ed.), *Surveillance as social sorting: Privacy, risk and digital discrimination* (pp. 1-9). New York: Routledge.

Lyon, D. (2003b). "Surveillance as social sorting: Computer codes and mobile bodies." In D. Lyon (Ed.), *Surveillance as social sorting: Privacy, risk and digital discrimination* (pp. 13-30). New York: Routledge.

Lyon, D. (2007). *Surveillance studies: An overview.* Malden: Polity Press.

Lyon, D. (2009). *Identifying citizens: ID cards as surveillance.* Malden: Polity Press.

Lyon, D. (2015). Surveillance after Snowden. Malden, MA: Polity.

Lyon, D. Haggerty, K.D., & Ball, K. (2012). "Introducing surveillance studies." In D. Lyon, K.D. Haggerty, & K. Ball (Eds.), *Routledge Handbook of Surveillance Studies* (pp. 1-11). Oxon: Routledge.

Maltby, M., Day, L., Hatcher, R.M., Tazzyman, S., Flowe, H.D., Palmer, E.J., Frosch, C.A., O'Reilly, M., Jones, C., Buckley, C., Knieps, M., & Cutts, K. (2016). Implicit theories of online trolling: Evidence that attention-seeking conceptions are associated with increased psychological resilience. *British Journal of Psychology 107*(3), 448-66.

Mann, S., Nolan, J. & Wellman, B. (2003). Sousveillance: Inventing and using wearable computing devices for data collection in surveillance environments. *Surveillance & Society 1*(3), 331-55.

Manning, P. (1992). Information technology and the police. In M. Tonry & N. Morris (Eds.), *Modern policing* (pp. 349-98). Chicago: University of Chicago Press.

Margulies, P. (2015). Defining "foreign affairs" in section 702 of the FISA amendments act: The virtues and deficits of post-Snowden dialogue on U.S. surveillance policy. *Washington and Lee Law Review, 72*(3), 1283-1306. Retrieved from http://login.ezproxy1.lib.asu.edu/login?url=http://search.proquest.com/docview/1756930756?accountid=4485

Marwick, A.E. (2012). The public domain: Social surveillance in everyday life. *Surveillance & Society (9)*4, (378-93).

Marx, G. T. (2004). Surveillance and society. In G. Ritzer, *Encyclopedia of social theory*. Thousand Oaks, CA: Sage Publications. Retrieved from http://web.mit.edu/gtmarx/www/surandsoc.html#References

Maryland.gov. (n.d.). Base realignment & closure: The security clearance and investigation process. Retrieved from http://www.brac.maryland.gov/documents/security%20clearance%20101%20 pp%20presentation.pdf

Mayring, P. (2000). Qualitative content analysis. *Forum: Qualitative Social Research Sozialforschung 1*(2). Retrieved from http://www.qualitative-research.net/index.php/fqs/article/view/1089/2385

McCrie, R.D. (2007). Security operations management. Burlington, MA: Butterworth-Heinemann. Retrieved from http://site.ebrary.com.ezproxy1.lib.asu.edu/lib/asulib/reader.action?docID=10160325

McDaniel, M. A. (1989). Biographical constructs for predicting employee suitability. *Journal of Applied Psychology, 74*(6), 964-970. doi:10.1037/0021-9010.74.6.964

McDaniel, M.A. (2016). Michael A. McDaniel curriculum vitae. Retrieved from http://www.people.vcu.edu/~mamcdani/Publications/McDaniel.pdf

McDaniel, M.A., Lees, C.A., & Wynn, H.A. (1995, May 16). *Personal credit information in screening for personnel reliability*. Paper presented at the Society for Industrial and Organizational Psychology, Orlando, FL. Retrieved from http://www.people.vcu.edu/~mamcdani/Publications/McDaniel,%20Lees,%20Wynn%20&%20Timm%20%281995,%20April%29%20SIOP%20credit.pdf

McDaniel, M. A., Whetzel, D. L., Schmidt, F. L., & Maurer, S. D. (1994). The validity of employment interviews: A comprehensive review and meta-analysis. *Journal of Applied Psychology, 79*(4), 599-616. doi:10.1037//0021-9010.79.4.599

Morville, P. (2005). *Ambient findablity*. Sebastopol, CA: O'Reilly Media.

Moynihan, D. (1997). Personnel security: Protection through detection. *Secrecy: Report of the Commission on Protecting and Reducing Government Secrecy* (pp. 75-94). Washington, DC: US Independent Agencies and Commissions. Retrieved from https://www.gpo.gov/fdsys/pkg/GPO-CDOC-105sdoc2/pdf/GPO-CDOC-105sdoc2-9.pdf

Nadesan, M.H. (2008). *Governmentality, biopower, and everyday life*. Florence, KY: Routledge.

The Navy Yard Tragedy. Hearing before the Committee on Homeland Security and Governmental Affairs of the United States Senate. 113th Cong. (2013).

NOAA. (2001). "Ames: Too Many Weaknesses." Retrieved from http://www.wrc.noaa.gov/wrso/security_guide/ames.htm#Aldrich%20Ames

Nomination of Hon. Katherine Archuleta. Hearing before the Committee on Homeland Security and Governmental Affairs of the United States Senate. 113th Cong. (2013). Retrieved from ProQuest Congressional Database.

O'Brien, C. M. (2010). Homeland security presidential directive-12, background investigations, and informational privacy rights. *Mississippi Law Journal*, *80*(1), 299-353.

Office of the Director of National Intelligence [ODNI]. (2016). Collection, use, and retention of publicly available social media information in personnel security background investigations and adjudications. Retrieved from https://www.odni.gov/files/documents/Newsroom/ Press%20Releases/SEAD5-12May2016.pdf

Oldham, J. (2011). You don't know what you don't know: Background investigations as a preemptive risk-management tool. *The Secured Lender, 67*(7), 44-46.

OPM IG Act, 113th Cong. Rec. H.R. 2860 (daily ed. January 14, 2014). Retrieved from ProQuest Congressional Database.

Orwell, G. (1950). *1984*. New York: Signet. (Original work published 1949)

Petersen, J.K. (2012). Handbook of surveillance technologies. 3rd ed. New York: Taylor and Francis.

Richards, N. M. (2008). Intellectual privacy. *Texas Law Review 87*(2), 387-445.

Richards, N. M. (2013). The dangers of surveillance. *Harvard Law Review 126*(7), 1934-1965.

Richards, N.M., & King, J.H. (2014). Big data ethics. *Wake Forest Law Review, (49)*2, 393-432.

Ritch, V. (1997). Background investigation for law enforcement. Durham, NC: Carolina Academic Press.

Rogers, R., Boals, A., & Drogin, E. Y. (2011). Applying cognitive models of deception to national security investigations: Considerations of psychological research, law, and ethical practice. *The Journal of Psychiatry & Law, 39*(2), 339-364. doi:10.1177/009318531103900209

S. 13-111 - Security Clearance Oversight and Reform Enhancement Act. (2013). Retrieved from ProQuest Congressional Database.

S. 113-257 -Preventing Conflicts of Interest with Contractors Act. (2014). Retrieved from ProQuest Congressional Database.

S. 113-276 - Security Clearance Oversight and Reform Enhancement Act. (2014). Retrieved from ProQuest Congressional Database.

S. 113-283 - Enhanced Security Clearance Act of 2014. (2014). Retrieved from ProQuest Congressional Database.

S. 434 - Security Clearance Accountability, Reform, and Enhancement Act of 2015. (2015). Retrieved from ProQuest Congressional Database.

S. 2683 - Clearance and Over-Classification Reform and Reduction Act. (2014). Retrieved from ProQuest Congressional Database.

Safeguarding our Nation's Secrets: Examining the National Security Workforce. Hearing before the Subcommittee on the Efficiency and Effectiveness of Federal Programs and the Federal Workforce of the Committee on Homeland Security and Governmental Affairs of the United States Senate. 113th Cong. (2013). Retrieved from ProQuest Congressional Database.

Safeguarding our Nation's Secrets: Examining the Security Clearance Process. Hearing before the Subcommittee on the Efficiency and Effectiveness of Federal Programs and the Federal Workforce of the Committee on Homeland Security and Governmental Affairs of the United States Senate. 113th Cong. (2013). Retrieved from ProQuest Congressional Database.

Saldana, J. (2011). *Fundamentals of qualitative research: Understanding qualitative research*. New York: Oxford University Press.

Schreier, M. (2014). Qualitative content analysis. In U. Flick (Ed.), *The SAGE handbook of qualitative data analysis* (pp. 170-184). doi: http://dx.doi.org/10.4135/9781446282243.n12

Schuessler, J. H., & Hite, D. M. (2014). Pre-employment screening for security risk: An exploratory study. *The Journal of Applied Business and Economics, 16*(1), 84-95.

Selyer, D.U. (2012). *Read, reason, write: An argument text and reader.* (11th ed.). New York: McGraw Hill.

Sidel, R. (2014, Sept. 18). Home Depot's 56 million card breach bigger than Target's. Retrieved from http://www.wsj.com/articles/home-depot-breach-bigger-than-targets-1411073571

Silverman, L. (2016, April 14). Using data to predict child abuse. Retrieved from http://www.marketplace.org/2016/04/14/world/using-data-predict-child-abuse-hot-spots

Slora, K.B., Joy, D.S, Jones, J. & Terris, W. (1991). The prediction of on-the-job violence. In J. Jones (Ed.), Preemployment honesty testing: Current research and future directions (pp. 171 – 185). New York: Quorum Books.

Smith, G.J.D. (2009). Empowered watchers or disempowered workers? The ambiguities of power within technologies of security. In K.F. Aas, H.O. Gundhus, & H.M. Lomell (Eds.), *Technologies of insecurity: The Surveillance of everyday life*. New York: Routledge-Cavendish.

Smith, G.J.D. (2012). Surveillance work(ers). In D. Lyon, K.D. Haggerty, & K. Ball (Eds.), *Routledge handbook of surveillance studies* (pp. 107-15). New York: Routledge.

Snowden, L., & Fuss, T. (2000). A costly mistake: Inadequate police background investigations. *Criminal Justice Studies, 13*(4), 359-375. doi:10.1080/1478601X.2000.9959600

Stalder, F. & Lyon, D. (2003). Electronic identity cards and social classification. In D. Lyon (Ed.), *Surveillance as social sorting: Privacy, risk and digital discrimination* (pp. 77-93). New York: Routledge.

Staples, W. G. (2000). *Everyday surveillance: Vigilance and visibility in postmodern life.* 2nd ed. Lanham: Rowman & Littlefield.

Stewart, S. (4 July 2013). The problems with background investigations. Retrieved from https://www.stratfor.com/sample/weekly/problems-background-investigations

Stoughton, J. W., Thompson, L. F., & Meade, A. W. (2015). Examining applicant reactions to the use of social networking websites in pre-employment screening. *Journal of Business and Psychology, 30*(1), 73-88. doi:10.1007/s10869-013-9333-6

"Surveillance metadata." (2014). Retrieved from http://whatis.techtarget.com/definition/surveillance-metadata

Surveillance. (2015). Retrieved from http://beta.merriam-webster.com/dictionary/surveillance

Surveillance - Google Search. (n.d.). Retrieved from https://www.google.com/search?q=surveillance&biw=1200&bih=654&source=lnms&tbm=isch&sa=X&ved=0CAcQ_AUoAmoVChMIpMGqnI3mxwIVDjeICh2h_gt5

Tenant screening – Applicant screening – Resident screening for landlords & apartment managers in the USA. (n.d). Retrieved from http://www.criminalhistorychecks.com/tenant-screening-resident-applicant-screening-for-landlords-apartment-managers/

Terpstra, D.E., Kethley, R.B., Foley, R.T., & Wanthanee, T.L. (2000). The nature of litigation surrounding five screening devices. *Public Personnel Management, 29*(1), 43-54.

United States Congress. (n.d.). S.1276 - Security Clearance Oversight and Reform Enhancement Act. Retrieved from https://www.congress.gov/bill/113th-congress/senate-bill/1276

United States Department of State [USDOS]. (2006, February 3). Adjudicative guidelines for determining eligibility for access to classified information. Retrieved from http://www.state.gov/ m/ds/clearances/60321.htm

United States General Services Administration. (n.d.). GSA Forms Library. Retrieved from http://www.gsa.gov/portal/forms/download/116382

United States Government Accountability Office [USGAO]. (1999). Inadequate personnel security investigations pose national security risks (Report No. NSIAD-00-12). Retrieved from http://www.gao.gov/ products/GAO/NSIAD-00-12

United States Government Accountability Office [USGAO]. (2000). Inadequate personnel security investigations pose national security risks (Report No. T-NSIAD-00-65). Retrieved from http://www.gao.gov/products/GAO/T-NSIAD-00-65

United States Government Accountability Office [USGAO]. (2013). Security clearances: Additional mechanisms may aid federal tax-debt detection (Report No. GAO 13-733). Retrieved from ProQuest Congressional Database.

United States Government Accountability Office [USGAO]. (2014a). Information security: Agencies need to improve oversight of contractor controls. (Report No. GAO 14-612). Retrieved from ProQuest Congressional Database.

United States Government Accountability Office. (2014b). Personnel security clearances: Additional guidance and oversight needed at DHS and DOD to ensure consistent application of revocation process. (Report No. GAO 14-640). Retrieved from ProQuest Congressional Database.

United States Office of Personnel Management [USOPM]. (n.d.). Background investigations. Retrieved from http://www.opm.gov/investigations/ background-investigations/

United States Office of Personnel Management [USOPM]. (n.d.). Frequently asked questions. Retrieved from https://www.opm.gov/faqs/topic/investigate/index.aspx?cid=56d6e92e-6e27-4b6a-8969-4a7a1bfba76d

United States Office of Personnel Management [USOPM]. (2011). Job family position classification standard for administrative work in inspection, investigation, enforcement, and compliance group, 1800. Retrieved from https://www.opm.gov/policy-data-oversight/classification-qualifications/classifying-general-schedule-positions/standards/1800/1800a.pdf

United States Office of Personnel Management [USOPM]. (n.d.). Questionnaire for national security positions. (OMB Publication No. 3206 0005). Retrieved from http://www.opm.gov/ forms/pdf_fill/SF86pdf

United States Office of Personnel Management [USOPM]. (n.d.). Questionnaire for non-sensitive positions. (OMB Publication No. 3206 0261). Retrieved from https://www.opm.gov/ forms/pdf_fill/sf85.pdf

United States Office of Personnel Management [USOPM]. (n.d.). Questionnaire for public trust positions. (OMB Publication No. 3206-0191). Retrieved from http://www.opm.gov/Forms/ pdf_fill/sf85p.pdf

@UnonimityUser. (2016, July 13). It's time to disrupt the advertising industry & take back control over our #privacy #security & #freedom tinyurl.com/unanimity # unanimity. Retrieved from https://twitter.com/UnonimityUser

Veiga, A. (2015, January 15). Economic recovery: Foreclosure rates drop to lowest level since Great Recession. Retrieved from http://www.csmonitor.com/Business/Latest-News-Wires/2015/0115/Economic-recovery-Foreclosure-rates-drop-to-lowest-level-since-Great-Recession

Wakeman, N. $30M settlement brings close to USIS saga. Retrieved from https://washingtontechnology.com/blogs/editors-notebook/2015/08/usis-settlement.aspx

Wald, M. (2012, August 12). Woman becomes first openly gay general. Retrieved from http://www.nytimes.com/2012/08/13/us/army-woman-is-first-openly-gay-officer-promoted-to-flag-rank.html?_r=0

Walker Rettberg, J. 2014. *Seeing ourselves through technology: How we use selfies, blogs and wearable devices to see and shape ourselves.* Bergen: Palgrave Macmillan.

Whitaker, R. (1999). *The end of privacy: How total surveillance is becoming a reality.* New York: New Press.

Wilson, J. M., Dalton, E., Scheer, C., & Grammich, C. A. (2010). *Police recruitment and retention for the new millennium: The state of knowledge*. Santa Monica, CA: RAND. doi:10.7249/mg959dojWoska 2007

Wise, J.M. (2002). Mapping the culture of control: Seeing through the Truman Show. *Television & New Media, 3*(1), 29-47.

Wise, J.M. (2005). “Assemblage.” In C.J. Stivale (Ed.), *Gilles Deleuze: Key concepts* (pp. 77-87). Montreal: McGill-Queen's University Press.

Woska, W.J. (2007). Legal issues for HR professionals: Reference checking/background investigations. *Public Personnel Management 36*(1), 79-89.

Wright, T.H. (1991). Pre-Employment background investigations. *The FBI Law Enforcement Bulletin*, *60*(11), 16-21.

Young, S. J. (Forthcoming). The Narrative of slipping through the cracks: Background investigations after Snowden. *Surveillance & Society*.

Young, S. J. (2015). Literacies for surveillance: Social network sites and background investigations. *Media and Communication, 3*(2), 88-97. Doi: 10.17645/mac.v3i2.266

Zureik, E. Theorizing surveillance: The case of the workplace. In *Surveillance as social sorting: Privacy, risk and digital discrimination* (pp. 31-56). New York: Routledge.

APPENDIX A

CONSTANCY (ABRIDGED)

- Continuous Assessment
  - Definition 4
  - Drawbacks/Limitations 18
  - Frequency 11
  - Gap between investigations 1
  - History 8
  - How it works 25
  - Programs 12
  - Real time 14
  - Role of Tech 13
  - Why used/justification - generic examples 21
  - Why used – specific examples 9

Sample Passages
Category - Continuous Assessment
Definition
• Control comes in the forms of continuous assessment (Deleuze, 1995, p. 182) • "constant monitoring checks worker activities and individual inducements provide incentives for compliance" (Lyon, 2007, p. 60)
Coding Rules
• Indication of continuous assessment • Continuous assessment with a tangible benefit
Examples
Definition 1. "The term \'continuous evaluation\', as defined in Executive Order 13467 (50 U.S.C. 3161 note), means reviewing the background of an individual who has been determined to be eligible for access to classified information at any time during the period of eligibility" (H.R. 5240, 2014; S. 2683, 2014). 2. "Continuous evaluation means reviewing the background of an individual who has been determined to be eligible for access to classified information (including additional or new checks of commercial databases, government databases, and other information lawfully available to security officials) at any time during the period of eligibility to determine whether that individual continues to meet the requirements for eligibility for access to classified information" (USGAO, 2013, p. 9) 3. Per EO 13467 and revised Federal Investigative Standards signed in 2012, "CE allows for a review at any time of an individual with eligibility or access to classified information, or in a sensitive position, to ensure that the individual continues to meet the requirements for eligibility" (*The Navy Yard Tragedy*, 2013, p. 64). 4. "The government has been working to establish automated systems, referred to generally as Continuous Evaluation (CE), to check government and commercial data sources on a more frequent or even continuous basis to flag issues of concern during the period between background investigations" (S. 113-283, 2014). **Drawbacks/Limitations** 1. These protections should include "standards for the protection of national security and promotion of fairness, transparency, and employee protections, including safeguards to preserve the rights and confidentiality of whistleblowers with respect to the operation of a continuous evaluation program and the operation of an insider threat program by a Federal agency" (H.R. 5240, 2014; S. 2683, 2014) 2. To curb abuse of CE, agencies must submit "Demographic information on each individual whose eligibility for access to classified information was changed as a result of information collected through the continuous evaluation program or insider threat program, including age, race, gender, and ethnicity. [And] a description of the mechanisms used to conduct the evaluations, including how individuals were selected,

whether the evaluations were randomized, and if so, the nature of the randomization, including the degree to which it was temporally randomized and the degree to which the selection of individuals subject to the program was randomized" (H.R. 5240, 2014; S. 2683, 2014)

3. "(B) any covered individual who is not a cleared individual is not subject to continuous evaluation or monitoring" (H.R. 490, 2015; H.R. 4022, 2014).
4. "In 2005, interestingly, a year before Ricky Elder enlisted in the Army, 2 years before Aaron Alexis enlisted in the Navy, and 7 years to the day before Ricky Elder's deadly attack, the Department of Defense testified to this Committee—and this was in June 2005—about the Automated Continuous Evaluation System, (ACES). And you all said that you were going to continuously evaluate the background and suitability of security clearances. Mr. Prioletti, in your opening—in your written statement—I did not hear you say it in your statement, but in your written statement you noted that 3 years earlier, in 2008—3 years later from the 2005 testimony you gave before this Committee, in 2008 President Bush directed by his Executive Order that an individual who has been determined to be eligible for or currently has access to classified information shall be subject to Continuous Evaluation. That was an Executive Order back in 2008" (*The Navy Yard Tragedy*, 2013, pp. 35-6).
5. Regarding CE, "I know we have heard today, ''We are working on this.'' I heard in response to an earlier question, ''We have an interagency working group. We are developing a concept of operations.'' I wrote this down. ''We are doing research.'' Again, this has been going on now for a decade. If you testified in 2005 it was going on in 2004, it may be more than a decade. So here we are. It is 5 years after the Executive Order, 8 years after this Committee heard about the plans, and we are dealing with the tragedy at the Navy Yard" (*The Navy Yard Tragedy*, 2013, p. 36).
6. "Senator PORTMAN. You were not here in this job 9 years ago when we heard that it was going to be in place by 2005. But you are here now, and so, one question I could ask you is: Why has it taken so long? And you might say, ''I do not know. I was not in charge.'' But you are in charge now, and you are saying that you are going to have this fully operational in 3 years. Is that correct?" (*The Navy Yard Tragedy*, 2013, p. 37)
7. "Mr. LEWIS. For the Automated Continuous Evaluation System as it currently stands, it is an operational system. It is still in a research and development mode, but it is an operational system. The limits right now—— Senator PORTMAN. I mean, when I say ''operational,'' I mean it actually would cover more than a small percentage of the people who are in between their clearances. You are talking about taking it from 3,600 up to 100,000. How many security clearances do you have at DOD? Mr. LEWIS. We have about 2.5 million people who are eligible and in access for classified information. Senator PORTMAN. So when are we going to cover these people? Mr. LEWIS. One of the things we are examining is can we expand the capability of the system to handle that larger volume, and that is a work in progress and something that we could report back to you on" (*The Navy Yard Tragedy*, 2013, p. 37).
8. Problems with CE are not necessarily funding, but "It is a question of having the right criteria in place to conduct the evaluations and then what we do with the data once it is generated from the system, how you evaluate that and how you take action based on that information" (*The Navy Yard Tragedy*, 2013, p. 37).
9. "A number of pilot studies have been initiated to assess the feasibility of select automated records checks and the utility of publicly available electronic information, to include social media sites, in the personnel security process. Although these pilots have identified actionable information, they indicate that retrieving, analyzing, and processing the data is likely to be resource intensive. More research is required to assess resource impacts and determine the most effective method to utilize publically available electronic information while protecting the privacy and civil liberties of those individuals being evaluated" (*The Navy Yard Tragedy*, 2013, p. 65).

10. Although shortening the time for periodic reinvestigations would help identify issues, "it also adds significant cost and resource burdens to federal agencies and to the federal adjudicators" (*The Navy Yard Tragedy*, 2013, p. 100).
11. “But the larger issue is how do we collect—how do we identify and collect relevant information that allows us to constantly adjust our perspective about cleared individuals and individuals who are in trusted positions? And that is really the challenge” (*The Navy Yard Tragedy*, 2013, p. 169).
12. “I hate to keep blowing the same horn, but the continuous evaluation process of not just collecting the information but having the staff available to evaluate the information and take action on that information, to me that is the real issue here” (*The Navy Yard Tragedy*, 2013, p. 169).
13. “Moreover, with the proposed implementation of continuous evaluation, the workload of agencies’ security offices could significantly increase, making it critical for agencies to have a high-quality clearance revocation process in place” (USGAO, 2014b, pp. 53-54).
14. “The Report explained that CE is an ambitious undertaking-- “Success of the CE program will depend on a fully-integrated solution across government, which will eliminate inefficiency and avoid the expenses of duplicative systems”--and the report also recognized the challenges and stated how much is yet to be done to reach that goal” (S. 113-283, 2014).
15. “Implementing a system for continuous evaluation is resource intensive, and poses genuine technical and procedural challenges” (S. 113-283, 2014).
16. “Currently there is no government-wide capability, plan or design present in the investigative community to operate a data-driven architecture to collect, store, and share relevant information” (S. 113-283, 2014).
17. “S. 1618 provides that random audits would not be required if more frequent automated checks of governmental and commercial records and data are being conducted with respect to the individual” (S. 113-283, 2014).
18. “This exemption for individuals who are the subject of more frequent automated checks is a key component of the program” (S. 113-283, 2014).

APPENDIX B

IDENTITY (ABRIDGED)

Articulated in context
- Adjudications 12
- Changeable 1
- People don't agree with determination 1
- Whole person 2

Obsessed with checking IDs
- Facts Exist 1
- ID Card 8
- ID Cards revoked for derogatory info 3

Ascribed by institutions
- Government-defined identities 8
- Identity based on adjudication 5

Biometric ID
- Fingerprints 6
- ID 1

IDs are self-generated and revealed information
- Public info and social media 10
- Self-reporting 20
- SSNs 1

Basis for assessment (also in risk)
- Access to food supply 1
- Alcohol 2
- Adjudications 1
- Citizenship 1
- Conduct 1
- Dishonesty 2
- Drugs 1
- Employment 5
- Financial problems 23
- High-risk individuals (also in prediction) 21
- Law enforcement 6
- Mental health 4
- Need firm identity 1

Sample Passages

Category - Identity

Definition

- Identities are relational, always involve others, and always change (Lyon, 2009, p. 12)
- Identities are articulated in particular contexts" (Barnard-Wills, 2012, p. 36), and in a subjectivist understanding, "identities are not fundamentally given by rather socially constructed" (Barnard-Wills, 2014, p.176)

Coding Rules

- Indications that an identity is a comparison to other others
- Idea that identities can change
- Resistance to identity

Examples

Adjudications

1. Once the investigator completes his or her work, OPM reviews the results package for completeness (and, when efforts to complete items were unsuccessful, reporting those efforts) and delivers it to the customer agency. The delivery is generally accomplished by electronic means to support electronic adjudication processes in place at Federal agencies" (*The Insider Threat*, 2013, p. 9).
2. "The decision that an individual should receive access to Classified information is ultimately, pursuant to Executive Order 12968, the exclusive responsibility of the head of the agency employing the individual, or his or her designee, following a National security adjudication (either by that agency or by a central adjudicative facility working on its behalf)" (*The Insider Threat*, 2013, p. 9).
3. "Background investigations for suitability and fitness examine character and conduct, and based upon all available information, we make an adjudicative decision concerning a person's suitability or fitness for employment or access to Classified information" (*The Insider Threat*, 2013, p. 12).
4. "Based upon all available information, a personnel security specialist makes an adjudicative decision concerning a person's suitability or fitness for employment, including access to facilities" (*The Insider Threat*, 2013, pp. 13-14)
5. "Adjudicative decisions are made by utilizing the whole-person concept, which is a careful weighing of available, reliable information about the person, past and present, favorable and unfavorable" (*The Insider Threat*, 2013, p. 16).
6. "Upon the receipt of derogatory information, the DOD consolidated adjudications facility would have made a determination does this clearance need to be suspended or revoked; is additional investigation required" (*DC Navy Yard Shooting*, 2014, p. 53).
7. "Well, as part of the reinvestigation process, the previous investigation is looked at for any derogatory information there, looking for trends, looking for ongoing concerns; and it is all part of a whole person concept where you look at what has happened in the person's life, what challenges they have faced, whether or not they have had issues with credit or alcohol, and that is part of the adjudicative process" (*DC Navy Yard Shooting*, 2014, p. 58).
8. In cases of "zestfully clean" results, "these cases, a computer reviews the file and has the ability to grant the clearance; since there is nothing for the first-level adjudicator to review, no such review takes place" (H. Rep, 2014, p. 30)
9. "Based upon all available information, a personnel security specialist makes an adjudicative decision concerning a person's suitability or fitness for employment, including access to facilities" (*Facility Protection*, 2013, p. 19).
10. "We, DHS, we adjudicate for that fitness determination. If that contractor has to have a security clearance, a National security clearance, that is conducted by the Department of Defense, Defense Security Service. They have jurisdiction over those investigations under the National Industrial Security Program. So, we do the fitness and we do the adjudication for the fitness to determine if that person is suitable, but any kind of

security clearance falls under the purview of the Department of Defense" (*Facility Protection*, 2013, p. 43).

11. "Based on the suitability criteria, an adjudicative determination is made whether the individual will promote the integrity and efficiency of the service" (*Facility Protection*, 2013, p. 54).
12. "When evaluating the information, DHS must apply the adjudicative criteria, which includes evaluating whether an individual's mental health condition adversely affects the individual's judgment and trustworthiness to safeguard classified information" (*Facility Protection*, 2013, p. 54).

Changeable

1. "You know, people are normal today. Look at this panel, they all look pretty normal, don't they? But they could flip out on you in a few years, particularly some. So we do need some mechanism to review people periodically as they take on new roles" (*DC Navy Yard Shooting*, 2014, p. 52).

APPENDIX C

MISCELLANEOUS (ABRIDGED)

Contents

Sample Passages
Category - Miscellaneous
Costs **Definition** • BIs and their associated procedures cost certain amounts.
Coding Rules • Passages include those that detail the costs of the BI.
Examples • **"**the Executive branch spends over $1 billion dollars on background investigations for suitability and security clearances, but could not yield Alexis's felony gun charges" (*The Insider Threat*, 2013, p. 1). • "It is important to note that all investigations are fixed-price products" (*DC Navy Yard Shooting*, 2014, p. 43). • "When USIS sent a completed case to OPM, it received 90% of its contract payment for that type of case. The remaining 10% was paid when the case was formally closed. The more cases USIS submitted to OPM, the more revenues it generated" (*DC Navy Yard Shooting*, 2014, p. 132). • "The Committee's investigation also identified bonuses received by USIS executives, noting a sharp increase when the alleged fraud began" (*DC Navy Yard Shooting*, 2014, p. 134). • "At no point did Mr. Calamia acknowledge that the reason OPM had found anomalously high numbers of reports released by very few quality reviewers was that USIS was dumping cases to maximize revenues" (*DC Navy Yard Shooting*, 2014, p. 135). "Senior USIS executives also benefitted financially since at least 75% of their personal bonuses were dependent on the company's meeting earnings and revenue targets" (*DC Navy Yard Shooting*, 2014, p. 137). • "Bill Mixon, the former President and CEO who set internal corporate revenue goals, obtained bonuses and stock totaling more than $1 million." (*DC Navy Yard Shooting*, 2014, p. 137). • The former Chief Financial Officer, who allegedly calculated the number of cases that needed to be reviewed and dumped to meet corporate goals, was awarded about $470,000 in bonuses (*DC Navy Yard Shooting*, 2014). • The former President of the Investigative Services Division, who allegedly instructed his employees to flush cases, obtained over $375,000 in bonuses (*DC Navy Yard Shooting*, 2014, p. 138).

- "Furthermore, we have reported that the federal government spent over $1 billion to conduct more than 2 million background investigations (in support of both personnel security clearances and suitability determinations for government employment outside of the Intelligence Community) in fiscal year 2011" (*DC Navy Yard Shooting*, 2014, p. 152).
- "Although Contractors are currently paid a set price for each investigation, not all investigations are the same. Some Top Secret investigations take substantially more time than others. Accordingly, one contractor recommended that OPM create tiers of prices based on the complexity of the case.93 Contractors also recommended that agencies improve their forecasting of required investigations to OPM, so that OPM can provide better forecasting to the contractors.94 OPM similarly expressed to the Committee that it is attempting to work with agencies in an effort to improve their forecasting" (H. Rep., 2014, p. 14)
- The Office of Personnel Management's Federal Investigative Services Division uses a Revolving Fund structure in which Federal agencies pay OPM for the different investigations each agency needs, both for its employees and for its contractors. As a former Missouri State auditor, I was shocked to learn that this fund has never been audited" (*Safeguarding Our Nation's Secrets: Examining the Security Clearance Process*, 2013, p. 3).
- "For its work for the Office of Personnel Management, USIS received more than $200 million last year" (*Safeguarding Our Nation's Secrets: Examining the Security Clearance Process*, 2013, p. 3).
- "To compensate, we have used the $3 million we have for non-trust fund work to maintain a modicum of oversight viability in the Revolving Fund programs, with special emphasis on the Federal Investigative Services program because of the national security implications" (*Safeguarding Our Nation's Secrets: Examining the Security Clearance Process*, 2013, p. 8).
- "in fiscal year 2012, DOD paid the Office of Personnel Management a total of $753 million for security clearance investigations and approximately $471 million for military service members, $30 million for DOD civilians, and $252 million for cleared industry" (*Safeguarding Our Nation's Secrets: Examining the Security Clearance Process*, 2013, p. 11).
- "Senator MCCASKILL. OK. So I need some kind of agreement here as to why this fund has never been audited. It is $1 billion a year. It is outrageous that it has never been audited. And so what is your rationale as to why this fund has never been audited?" (*Safeguarding Our Nation's Secrets: Examining the Security Clearance Process*, 2013, p. 15).
- "Mr. MILLER. My understanding is OPM—we support the current request by the OIG for Revolving Fund dollars to support audits in the future. The issue in the past was there was not a legal basis for Revolving Fund dollars to be given to the IG for audit purposes. We welcome the IG's oversight. Senator MCCASKILL. Well, these are all public dollars. Mr. MILLER. They are public dollars. They are not appropriated dollars." (*Safeguarding Our Nation's Secrets: Examining the Security Clearance Process*, 2013, p. 15).
- Mr. MILLER. It was absolutely auditable. The issue was whether Revolving Fund dollars could be given to the IG to resource additional personnel to actually conduct the audit. They could have used appropriated dollars at any time to audit the Revolving Fund." (*Safeguarding Our Nation's Secrets: Examining the Security Clearance Process*, 2013, p. 15).
- "I am curious about paying for these for contractors; $250 million, I think Mr. Lewis said, was paid just for security clearance for contractors in 1 year" (*Safeguarding Our Nation's Secrets: Examining the Security Clearance Process*, 2013, p. 25).
- "We do not charge contractors for the costs of their security clearance. Part of our budget is the cost for funding cleared contractors in industry, and that is what that $252

million was for fiscal year 2012." (*Safeguarding Our Nation's Secrets: Examining the Security Clearance Process*, 2013, p. 25).

- "We have done extensive research as to what is the most cost-effective way to pay for security clearance within the Department. The analysis shows that if we were to allow the contractors to build the cost of clearances into the contract then they would add overhead on the management of that. So the most cost-effective way was to manage it from the Department, we pay those costs, because we pay it either way" (*Safeguarding Our Nation's Secrets: Examining the Security Clearance Process*, 2013, pp. 25-6).
- "we are paying USIS several hundred million dollars a year to do background checks, and we are paying them $45 million a year to do the office work" (*Safeguarding Our Nation's Secrets: Examining the Security Clearance Process*, 2013, p. 27).
- OPM's OIG has a $24 million appropriation, but $21 million goes to retirement, healthcare, and life insurance trust. That leaves 3 million for FIS, other revolving fund programs like Human Resources Solutions and USAJOBS, and other non-trust fund programs like flexible spending and dental/vision insurance (*Safeguarding Our Nation's Secrets: Examining the Security Clearance Process*, 2013, p. 39).
- The OIG seeks one third of one percent of the Revolving Fund Budget for audits/oversight. (*Safeguarding Our Nation's Secrets: Examining the Security Clearance Process*, 2013, p. 40).
- "the fiscal year 2012 base price for a top secret clearance investigation conducted by OPM was $4,005, while the base price of a secret clearance was $260." (*Safeguarding Our Nation's Secrets: Examining the Security Clearance Process*, 2013, p. 51).
- From FY13 to FY15, sing contractors for the support services contract produces a $17.85-million-dollar cost savings as opposed to using Federal equivalents, especially since contractors can easily reduce the number of employees with work load fluxuation (*Safeguarding Our Nation's Secrets: Examining the Security Clearance Process*, 2013, p. 67).
- OPM charges $4005 for an SSBI, but other agencies like the NSA using the same investigator cost $2400 (40% less) because of the costs of maintaining the process overall – OPM is the designated, government-wide agency. The NSA price does not account for those cots. OPM-FIS is the only investigative agency that has to operate on a full cost recovery basis from the revolving fund. Other costs for operating expenses are $47.9 M for infrastructure and overhead, $263.9 M for federal staff, $15.5 M for facilities, $456.3 for investigative contracts, $47.9 M for FBI fees, $16.6 M for travel, $10.8 M for supplies, and $100.5 IT/O&M and Investment. (*Safeguarding Our Nation's Secrets: Examining the Security Clearance Process*, 2013, p. 69).
- "By far, the largest increase in government-wide efficiency and resulting cost benefit occurred when OPM reduced the time required to perform the investigation process from an average of 145 days in FY05 to 36 days in FY12....OPM has saved the federal government over $25 billion because the improved investigation timeliness has allowed agencies to clear individuals faster and put them to work at the jobs they were hired to do" (*Safeguarding Our Nation's Secrets: Examining the Security Clearance Process*, 2013, p. 73).
- Cost of employee/contractor breakdown (*Safeguarding Our Nation's Secrets: Examining the Security Clearance Process*, 2013, pp. 84-87).
- From FY13 to FY15, sing contractors for the support services contract produces a $21.54-million-dollar cost savings (*The Navy Yard Tragedy*, 2013, p. 109)
- In order to address 2014 sequestration budget reductions, agencies were asked to evaluate whether clearances were needed and terminate access if determined clearances were not necessary (*The Navy Yard Tragedy*, 2013, p. 125).
- "I can understand that if you are looking at the building that houses the public employees for the Farm Service Agency in Watford City, North Dakota, you might not want to put any kind of screening device. But for a building that houses and employs—where thousands of employees come, it seems like there might be some cost/benefit in

safety in looking at electronic surveillance. There might be some cost/benefit in providing law enforcement- trained people at the front to engage, that we might look at those kinds of procedures. And I do not hear that today" (*The Navy Yard Tragedy*, 2013, p. 161).

- Physical security guard contracts "are not non-lucrative contracts" (*The Navy Yard Tragedy*, 2013, p. 165).
- "The drawback to screening every employee coming through is the negative impact on mission accomplishment, and there are facilities where there are 10,000 employees coming through often in roughly the same window, and screening every single employee would be disruptive to getting the work done. And that is the balance, factoring in cost and mission accomplishment against screening every employee" (*The Navy Yard Tragedy*, 2013, p. 165).
- "conducting background investigations is costly. We found the Federal Government spent over $1 billion to conduct background investigations in fiscal year (FY) 2011" (*Safeguarding Our Nation's Secrets: Examining the National Security Workforce*, 2013, p. 9).
- "And by the way, the cost of this is growing, too. From 2001 to 2011, that 10-year period, until a couple years ago, the cost went from $4.7 billion to $13.6 billion a year. So now, $13.6—$13.4—$13.36 billion a year in simply costs associated with storing this vast amount of information. And by the way, that does not include the over $1 billion needed every year just to clear the personnel authorized to have contact with this information, or to work with this material" (*Safeguarding Our Nation's Secrets: Examining the National Security Workforce*, 2013, p. 17).
- "The fiscal year 2014 base price for an initial top secret clearance investigation conducted by OPM is $3,959 and the cost of a periodic reinvestigation is $2,768. The base price of an investigation for a secret clearance is $272. If issues are identified during the course of an investigation for a secret clearance, additional costs may be incurred" (*Safeguarding Our Nation's Secrets: Examining the National Security Workforce*, 2013, p. 58).

Definitions

Definition

- Terms are defined in certain ways.

Coding Rules

- Passages define terms used during discussions of the BI.

Examples

- Definition of reciprocity: "agencies do not consistently and comprehensively track the reciprocity of personnel security clearances, which is an agency's acceptance of a background investigation or clearance determination completed by any authorized investigative or adjudicative agency" (*The Insider Threat*, 2013, p. 22).
- Definitions of terms are listed on PDF page 5-6 (H.R. 490, 2015; H.R. 4022, 2014).
- Regarding position designation oversight, "Oversight methodology includes assessment of agency policy guidance, confirmation that personas making position designation determinations are properly trained, and assessment of position designation determination documentation" (*Safeguarding Our Nation's Secrets: Examining the National Security Workforce*, 2013, p. 87).
- "For employment in a civilian position outside the competitive service or a position with a government contractor, the term 'fitness' is generally used instead of 'suitability'" (S. 113-283, 2014).
- "The term 'covered individual' is defined to mean an individual who has been determined eligible for access to classified information or to hold a sensitive position" (S. 113-283, 2014).
- "The term 'periodic reinvestigations' is defined to mean investigations conducted periodically, with a frequency as required by the Director of National Intelligence, for

the purpose of updating a previously conducted security background investigation" (S. 113-283, 2014).

- "the term 'enhanced personnel security program' means a program implemented by an agency at the direction of the Director of National Intelligence under subsection" (S. 113-283, 2014).
- "The term \'continuous evaluation\', as defined in Executive Order 13467 (50 U.S.C. 3161 note), means reviewing the background of an individual who has been determined to be eligible for access to classified information at any time during the period of eligibility" (H.R. 5240, 2014; S. 2683, 2014).

APPENDIX D

PREDICTION (ABRIDGED)

- How to predict
  - Alert 4
  - Continuous evaluation 2
  - Credit 1
  - More people, more risk 1
  - Processes 7
  - Random 1
  - Warning Signs/ Flagging/ High Risk Designations 19
- Technology and Prediction
  - More technological monitoring = prediction 5
- Probabilities and Prediction
  - Belief in prediction 15
  - No belief in prediction 10
  - Only past account – skeptic 3

Sample Passages
Category - Prediction
Subcategory - How to Predict **Definition** • The coding behind "dividuals" is important because "the codes are supposed to contain the means of prediction, of anticipating" events, conditions, and behaviors yet to happen (Lyon, 2003, p. 24) • The individual is reduced to a statistic by shifting surveillance from observation to prediction and by using statistics to infer profiles, the subject is desconstructed and not directly under scrutiny (Zureik, 2003, p. 39) • Individuals reduced to "numbered bodies of coded 'dividual[s]' (Deleuze, 1995, p. 182) • Dividuals create categories of people (and not particular individuals) which, like the idea of new penology, classifies groups into levels of access or dangerousness (Lyon, 2007, p. 61) • "Data generated through surveillance techniques produce 'types'" that are at "risk" for behavior (Staples, 2000, p. 6) • This moves punishment from the individual deviant to the overall "type" (Staples, 2000, p. 6).
Coding Rules • Indication of attempting to identify risks before they occur for certain groups of people • Discussions on "types" of people likely to (not) do something • Identity refers to a group of people rather than particular individuals • Discussion of statistics on groups of people rather than of any one person in particular. • Indications of "types" of people
Examples
Alert 1. "The OPM Background Investigation process must be capable of flagging high-risk individuals holding clearances and alert case officers of situations requiring review before any adverse consequence takes place" (Enhanced Security, 2013). 2. "Army officials explained that there is a resignation code in their human capital database, but that code covers all resignations for any reason, and there may or may not be a remark on the agency's personnel action form (known as an SF-50) that would relate the resignation to a security clearance issue" (USGAO, 2014b, p. 48) 3. "Moreover, Army officials explained that if an individual were removed as a result of a security clearance revocation, the removal code could be attributed to failing to meet any one of several conditions of employment, if maintaining eligibility for a security

clearance was one of the requirements listed in an individual's position description" (USGAO, 2014b, p. 48).

4. "An official from the Office of the Under Secretary of Defense for Personnel and Readiness explained that the separation codes applied for military personnel are similarly broad in nature, and would include separations for reasons other than revocation of a security clearance" (USGAO, 2014b, p. 48).

Continuous

1. Regarding continuous evaluation, "I see from the technical report on the project that there have been some pilot projects. You have 3,600 personnel records that have been searched. And it is working. Sixty-five of those 3,600 ended up having clearances suspended or revoked due to derogatory discoveries. Your search algorithms have found problems. But 3,600 people is a drop in the bucket when we have over 5 million people with security clearances" (*The Navy Yard Tragedy*, 2013, p. 36).
2. "Senator TESTER. Brenda, I want to get back to the rules and codification of them. Do you think there is a worth in codifying the guidance, the updated guidance along with quality controls, periodic reviews, guidance beyond the 24 months proposed in the rule?" (*Safeguarding Our Nation's Secrets: Examining the National Security Workforce*, 2013, p. 26)

APPENDIX E

RISK (ABRIDGED)

Types of risks - 218

- Adjudicative guidelines 7
- Alcohol 7
- Association 2
- BIs 16
- Can't get all 3
- Communication 1
- CE 4
- Contractors 1
- Credit 34
- Damage potential 2
- Derogatory info 1
- Documents missing 8
- Drugs 4
- Education 4
- Employment 16
- Facilities 4
- Foreign 10
- Inside threats 5
- Internet 9
- Law enforcement 30

Risk -647

- Lifestyle 6
- Mental / emotional 8
- Prohibited items 1
- Residence 5
- Sources 11
- Subjects 13
- Terrorism 5
- Under-reporting 1

Risk communication systems - 389

- Adjudication 37
- Director of National Intelligence (DNI) 18
- Determination of clearance 3
- Facilities 12
- Investigator 17
- Level 45
- OPM 47
- Problems 19
- Reciprocity 6
- Rules, regulations, laws 127
- Steps of clearance 58

Basis for assessment 40

- Access to food supply 1
- Adjudications decide suitability 1
- Alcohol 1
- Citizenship 1
- Conduct 1
- Dishonesty is bad 2
- Drugs 1
- Employment problems 4
- Financial problems 7
- High-risk individuals 13
- Law enforcement 5
- Mental health 2
- Need identity 1

Sample Passages

Category - Risk

Types of Risks

Definition

- "Risk refers to external danger, such as a natural disaster, technological catastrophe, or threatening behavior by human beings" (Ericson & Haggerty, 1997, p. 3).
- In a risk society, "risk communication formats are the focal point for an institutions selection and definition of risks" (Ericson & Haggerty, 1997, p. 9).
- To know what a risk is, is to know the institutional discourse around the risk - how it is classified, what it means, and how it should be responded to (Ericson & Haggerty, 1997)
- Surveillance provides the data for risk assessments (Barnard-Wills, 2012, p. 178) and risk types (Staples, 2000)

Coding Rules

- Discussions of different types of risks - what are identified by the documents as being risks?
- Discussions of how to determine risk (i.e., investigative and adjudicative criteria)
- Discussion of where the background information comes from
- What is required for the SF-86

Examples

Adjudicative guidelines

1. "Well, as part of the reinvestigation process, the previous investigation is looked at for any derogatory information there, looking for trends, looking for ongoing concerns; and it is all part of a whole person concept where you look at what has happened in the person's life, what challenges they have faced, whether or not they have had issues with credit or alcohol, and that is part of the adjudicative process" (*DC Navy Yard Shooting*, 2014, p. 58).
2. "In adjudicating eligibility for access to classified information or assignment to sensitive duties, the Department [of Defense] applies the Presidentially-approved Federal "Adjudicative Guidelines for Determining Eligibility for Access to Classified Information" which apply to civilian and military persons, consultants, contractors, and others who require access to classified information" (*Safeguarding Our Nation's Secrets: Examining the Security Clearance Process*, 2013, p. 91).
3. Decisions about revoking clearances are also based on the "Adjudicative Guidelines for Determining Eligibility for Access to Classified Information" (*Safeguarding Our Nation's Secrets: Examining the Security Clearance Process*, 2013, p. 91).
4. "What is the information that we collect and measured against the 13 adjudicative standards, and does it all flow right? That is all part of it and then the accountability" (*The Navy Yard Tragedy*, 2013, p. 31).
5. Adjudicator productivity does not depend on how many clearances granted or denied, and there is no incentive either way (*The Navy Yard Tragedy*, 2013, p. 132).
6. "Following the background investigation comes the adjudication stage, in which the sponsoring agency assesses the information collected and determines whether to grant to the individual a security clearance or allow the individual to occupy the sensitive position" (S. 113-283, 2014).
7. "The vetting of government personnel generally involves two distinct steps: investigation and adjudication" (S. 113-283, 2014).

Alcohol

1. "Well, as part of the reinvestigation process, the previous investigation is looked at for any derogatory information there, looking for trends, looking for ongoing concerns; and it is all part of a whole person concept where you look at what has happened in the person's life, what challenges they have faced, whether or not they have had issues with credit or alcohol, and that is part of the adjudicative process" (*DC Navy Yard Shooting*, 2014, p. 58).

2. Alexis, “He broke his foot jumping off stairs while intoxicated, he fired a gun into his ceiling and through the apartment above, he fired a bullet through the wall of his room, he quit his job, and he complained that individuals were using a microwave machine to send vibrations into his body” (H. Rep., 2014, p. 2).
3. “In fact, postings of people drinking when they were under age might be on the Internet” (H. Rep., 2014, p. 37).
4. “This form, three pages of instructions, seven pages where you live, five pages of names, 17 pages of employment, four pages of military, 29 pages on relationship, 21 pages on foreign activity, two pages on emotional health, seven pages on Police records, 11 pages on drug and alcohol, eight pages on financial records, five pages on associations, and three signature pages” (*The Navy Yard Tragedy*, 2013, p. 21).
5. “A security investigation begins when the individual, at the request of the sponsoring agency, submits an application in which the individual provides detailed information on a broad range of topics, including: personal history, identity of relatives and friends, foreign contacts and activities, criminal and legal record, any financial or tax difficulties, use of drugs and alcohol, and other matters” (S. 113-283, 2014).
6. “Background investigations for suitability and fitness examine character and conduct behaviors, such as criminal history, alcohol and drug use, and employment history, among others” (*Facility Protection,* 2013, p. 19).
7. “We look at things like conduct in past employment, criminal history, alcohol and drug abuse, that type of thing; whether or not the person has engaged in any activities that are contrary to U.S. interests and so forth. With respect to contractors, they undergo the fitness” (*Facility Protection,* 2013, pp. 42-3).

APPENDIX F

SOCIAL SORTING (ABRIDGED)

- Databases
    - Adjudication 2
    - Difference between crimes 1
    - Sorting as tool for acceptance/denial 3
    - Tech 19
- Codes
    - Facilities 4
    - Law enforcement 2
- Consumer surveillance
    - Credit use 23

Sample Passages
Category - Sorting
Databases **Definitions** • Relies on searchable databases "to determine who should be target for special treatment, suspicion, eligibility, inclusion, access" (Lyon, 2003, p. 20) • "Social sorting refers to a variety of surveillance practices that create various databases and have access to others--public services, police, intelligence, business, consumers - in order to categorize people for different treatment" (Gordon, 2011, p. 167).
Coding Rules • Evidence that information from databases is used for determining outcomes
Examples
Adjudication 1. Once the investigator completes his or her work, OPM reviews the results package for completeness (and, when efforts to complete items were unsuccessful, reporting those efforts) and delivers it to the customer agency. The delivery is generally accomplished by electronic means to support electronic adjudication processes in place at Federal agencies" (*The Insider Threat*, 2013, p. 9). 2. In cases of "zestfully clean" results, "these cases, a computer reviews the file and has the ability to grant the clearance; since there is nothing for the first-level adjudicator to review, no such review takes place" (H. Rep., 2014, p. 30). **Difference between crimes** 1. "And as I sat here, I could not think that the chairman and I were just talking about our various districts and I think about the people on my block. I live not too far from the Ravens Stadium in Baltimore, and I have said this many times, if somebody in my block, and there are people there who, if they stole a bike, they get a record for a lifetime. If they steal a bike, $150 bike. Record, lifetime, where they may won't be able to get jobs, won't be able to live in certain places, won't be able to get certain education opportunities like scholarships and whatever. And then when I look at stuff like this, where people are not doing their jobs and I am sure the investigation will reveal what it will reveal, but I am sure there are some criminal activity here (*DC Navy Yard Shooting*, 2014, pp. 76-7).

APPENDIX G

SURVEILLANT ASSEMBLAGE (ABRIDGED)

- Expanded collection, agency, and scrutiny
    - Multiple sources of information - 43
- Multiple locations
    - Locations - 7
- Power not limited to place
    - Reciprocity - 15

Sample Passages
Category – Surveillance Assemblage
Expanded collection, agency, and scrutiny **Definition** • Seemingly unrelated data flowing from multiple sources that are "reassembled and scrutinized in the hope of developing strategies of governance, commerce and control" (Haggerty & Ericson, 2000, p. 613). • Surveillant assemblages expand surveillance from the idea of one watcher to a larger network and flow of information coming from multiple places (Haggerty & Ericson, 2000) • It is more of a distributed collection of information which uses "techniques derived from military, administrative, employment, policing and marketing practices" (Lyon, 2007, p. 95).
Coding Rules • Evidence of data coming from multiple sources
Examples
Multiple sources of info 1. "There are a number of on-going pilot studies to assess the feasibility of selected automated record checks and the utility of publicly-available electronic information to include social media sites in the personnel security process" (*The Insider Threat*, 2013, p. 16). 2. "C.E., as envisioned in the reformed security clearance process, includes automated record checks of commercial databases, Government databases, and other information lawfully available" (*The Insider Threat*, 2013, p. 16). 3. "There are automated systems that would allow us to compare various identity checks and data with the answers subject provide in the SF86 Security Clearance Questionnaire, which could help identify false or omitted information" (*The Insider Threat*, 2013, p. 33). 4. "Currently, investigators do not review subjects' social media or traditional media records. Those sources of information should be reviewed in appropriate circumstances to conduct more thorough investigations" (*DC Navy Yard Shooting*, 2014, p. 34). 5. Social media is not a tool that is currently being used; however, it is being studied. And one of the challenges of using social media is validating the information that is available on the Web" (*DC Navy Yard Shooting*, 2014, p. 58). 6. "Well, as part of the reinvestigation process, the previous investigation is looked at for any derogatory information there, looking for trends, looking for ongoing concerns; and it is all part of a whole person concept where you look at what has happened in the person's life, what challenges they have faced, whether or not they have had issues with credit or alcohol, and that is part of the adjudicative process" (*DC Navy Yard Shooting*, 2014, p. 58) 7. "Mr. FARENTHOLD. As part of the background check, do you all Google the person? Ms. ARCHULETA. The use of social media is a technique that is being reviewed right now and recommendations have been provided by the DNI and supported by OPM" (*DC Navy Yard Shooting*, 2014, p. 60)

8. "Mr. FARENTHOLD. Just checking somebody's credit score on a regular basis or polling databases to see if somebody's name pops up" (*DC Navy Yard Shooting*, 2014, p. 61).
9. "(A) on a continual basis, access Federal, State, and local government and commercially available information, including financial credit history, currency transactions, court records, traffic violations, arrest records, terrorist and criminal watch lists, foreign travel, and online social media" (H.R. 490, 2015).
10. "Congress should consider the creation of a system providing for continuous evaluation or monitoring of federal personnel holding security clearances through which federal agencies will have real-time access to critical information relevant to background check investigations, including arrest records, court records, financial credit history, currency transactions, foreign travel, social media, and terrorist and criminal watch lists" (*DC Navy Yard Shooting*, 2014, p. 140).
11. "(6) enhance methods for reducing or eliminating manual processes with respect to security clearance background investigations, and automating and integrating the elements of such investigations and adjudication processes, including—"(A) the security clearance application process; " "(B) field investigator reporting; (C) investigation case management; (D) the collection, analysis, storage, retrieval, and transfer of data and records; "(E) the submission of any background investigation report to an agency for adjudication; and (F) records management for security clearance adjudication determinations" (H.R. 490, 2015).
12. "(A) on a continual basis, access Federal, State, and local government and commercially available information, including financial credit history, currency transactions, court records, traffic violations, arrest records, terrorist and criminal watch lists, foreign travel, and online social media" (H.R. 490, 2015).
13. "Congress should force OPM's investigative practices into the twenty-first century by allowing investigators to use the internet and social media sources in particular for the first time." (H. Rep., 2014, p. 3).
14. "recent technologies and the rise of social media now allow for these investigations to encompass even more information about applicants while still allowing the investigations to be completed in a timely manner" (H. Rep., 2014, p. 3).
15. "Recommendation 38 stated: We recommend that the vetting of personnel for access to classified information should be ongoing, rather than periodic. A standard of Personnel Continuous Monitoring should be adopted, incorporating data from Insider Threat programs and from commercially available sources, to note such things in credit ratings or any arrests or court proceedings" (H. Rep., 2014, pp. 33-4).
16. "The continuously updated information should include information relating to criminal or civil legal proceedings to which the individual with a clearance is a party. Information on financial difficulties the individual might encounter after receiving the initial clearance should also be under continuous evaluation" (H. Rep., 2014, p. 35).
17. "These three social media and search sites [Twitter, Facebook, and Google], among others, contain a treasure trove of information about their users. And the Americans that hold, or will apply for, federal security clearances use them frequently" (H. Rep., 2014, p. 36).
18. "Use of the internet is permissible for lead purposes" (H. Rep., 2014, p. 36).
19. "This restrictive policy keeps nearly every piece of information on a Subject's social networking site outside the reach of security clearance investigators. Given that tens of millions of Americans visit social media sites daily, an updated policy that appropriately considers privacy concerns would allow federal investigators to pull information about Subjects from of these and other websites" (H. Rep., 2014, pp. 36-7).
20. "It's not collecting it, it's not finding it, it's then doing the analysis, because when you run an investigation you shouldn't be incorporating information that isn't true about the subject in that investigation" (H. Rep., 2014, p. 37).
21. "Committee is considering legislation to require OPM to allow its background investigators to use social media sites and other Internet resources to develop

information on Subjects under investigation for a possible clearance" (H. Rep., 2014, p. 37).

22. "One possibility would be to have the investigator search for publicly available information on a Subject, and then confirm the veracity with the Subject and his or her friends and family. Another possibility would ask a Subject to disclose the social media and other Internet sites he or she visits on a regular basis on the SF-86" (H. Rep., 2014, p. 37) – although an OPM official stated" I have not heard any dialogue about adding individual social media sites to the SF-86" (H. Rep., 2014, p. 38).
23. By allowing internet use, "federal investigators, and ultimately the adjudicators, will be able to develop a more complete picture of the Subjects under consideration for a security clearance than currently exists today" (H. Rep., 2014, p. 38).
24. "The area that I think you are most concerned about is the social media or publicly available electronic information, and that is where the research is being done, Senator. We have to find that balance between the civil liberties and privacies of a U.S. citizen versus national security interests. That is where we are doing it. I do not have, as a representative of the ODNI, the luxury of going into a social media or publicly available database, pull information out of there, and submit it as being the truth. The government has a responsibility, an obligation to every one of its citizens to ensure that the information is true and accurate before we use it in the adjudicative process" (*The Navy Yard Tragedy*, 2013, p. 29).
25. "Well, I know my time is up, but I can tell you that obviously when our teenagers go online and get important information on social media and yet we are not going to use it to find out that someone is involved in something, I think that is a little hard to believe. We need to take a commonsense approach to this" (*The Navy Yard Tragedy*, 2013, p. 29).
26. "every parent on this panel who deals with social media knows if you want to know what your kid is doing, go out on social media. You may think that does not have the veracity of a court record, but I can tell you, as somebody who has looked at court records repeatedly doing background checks, it certainly does. A picture is worth a thousand words, and it is heartbreaking" (*The Navy Yard Tragedy*, 2013, p. 30).
27. Regarding social media, "The more information we can gain, the more enlightened the decision can be on whether or not to grant the access to classified or access to a sensitive position" (*The Navy Yard Tragedy*, 2013, p. 40).
28. "One of the obvious sources, potential sources of information, is social media or publicly available electronic information. What I referred to in terms of the research was the idea that we need to look at both what possible sources of information are out there, which ones would be of most benefit to provide adjudicatively relevant information for the access to classified information, and how do we do that in the best way that protects both the personal rights of the individual as well as the veracity and the coverage of the U.S. Government" (*The Navy Yard Tragedy*, 2013, p. 40).
29. "A number of pilot studies have been initiated to assess the feasibility of select automated records checks and the utility of publicly available electronic information, to include social media sites, in the personnel security process... More research is required to assess resource impacts and determine the most effective method to utilize publically available electronic information while protecting the privacy and civil liberties of those individuals being evaluated" (*The Navy Yard Tragedy*, 2013, p. 65)
30. "Field investigations include work such as conducting Enhanced Subject Interviews (ESI), obtaining personal testimony from a variety of source types, conducting record searches, and reporting all information obtained. Specific work requirements include case control/assignment, performance to investigative scope and coverage, reports of investigation, management of inventory, and quality control of deliverables to ensure quality standards are met" (*The Navy Yard Tragedy*, 2013, pp. 121-2).
31. "Several agencies are conducting pilot programs on the use of publically available electronic information/social media to assess the utility of the information available, the resources required to include such checks as part of a security clearance betting

program, filtering the data validation of the information, and to identify the measures required to ensure the privacy and civil liberties of the individuals" (*The Navy Yard Tragedy*, 2013, p. 126).

32. "The use of automated searches and social media enhance an adjudication's ability to make a well information eligibly determination" (*The Navy Yard Tragedy*, 2013, p. 126).
33. "The social media pilot program has shown that information taken from social need sites should be "validated rather than accepted as fact" (*The Navy Yard Tragedy*, 2013, p. 126).
34. Electronic data is not inherently different from any other data collected during a background investigation. Regardless of the source, noteworthy information must be explored to verify the accuracy of the information, develop details regarding the issues, and identify sources that support or mitigate the issue. In the end, decisions to grant or deny a clearance are not made on unsubstantiated data, but no a compilation of data from multiple sources that present a detailed, "whole person" view of the subject of investigation" (*The Navy Yard Tragedy*, 2013, p. 126).
35. Before physical security comes into play, it is important to have well-screened employees working on the physical security of a building and being employed by the Federal government. "Continuous evaluation" which can provide information such as recent arrest convictions from anywhere on a timely basis, and the "Insider Threat" initiative which "seeks to complement the continuous evaluation concept by incorporating data from a broad set of data sources to identify problematic behavioral trends will help identify those that need to have clearance or authorization revoked" (*The Navy Yard Tragedy*, 2013, p. 225).
36. CE "involves automated data checks from sources such as credit checks, social media, and personnel records to provide near-real-time notification of relevant information to help identify potential risks to national security" (USGAO, 2014b, p. 2).
37. "continuous evaluation of employees and contractors who are eligible for access to classified information, which involves automated data checks from sources such as credit checks, social media, and personnel records" (USGAO, 2014b, p. 2).
38. "The process begins with adverse information that can come from a variety of sources, including but not limited to individual self-reporting, federal or contract investigators who are conducting an investigation, Inspector General channels, hotlines, civilian law enforcement agencies, and reporting by persons such as security officers" (USGAO, 2014b, p. 12).
39. "A security investigation begins when the individual, at the request of the sponsoring agency, submits an application in which the individual provides detailed information on a broad range of topics, including: personal history, identity of relatives and friends, foreign contacts and activities, criminal and legal record, any financial or tax difficulties, use of drugs and alcohol, and other matters" (S. 113-283, 2014).
40. The enhanced security review "must integrate relevant information from various sources, including government and commercial data sources, consumer reporting agencies, and social media, including the types of information that are relevant for consideration in a background investigation" (S. 113-283, 2014).
41. The enhanced security review "must integrate relevant information from various sources, including government and commercial data sources, consumer reporting agencies, and social media, including the types of information that are relevant for consideration in a background investigation" (S. 113-283, 2014).
42. "(1) Sources of information.--The enhanced personnel security program of an agency shall integrate relevant information from various sources, including government, publicly available, and commercial data sources, consumer reporting agencies, social media, and such other sources as determined by the Director of National Intelligence" (S. 113-283, 2014).
43. "information relating to any criminal or civil legal proceeding; (B) financial information relating to the covered individual, including the credit worthiness of the covered individual; (C) public information, including news articles or reports, that includes

relevant security or counterintelligence information about the covered individual; (D) publicly available electronic information, to include relevant security or counterintelligence information on any social media website or forum, that may suggest ill intent, vulnerability to blackmail, compulsive behavior, allegiance to another country, change in ideology, or any other information that may suggest the covered individual lacks good judgment, reliability or trustworthiness; and (E) data maintained on any terrorist or criminal watch list maintained by any agency, State or local government, or international Organization" (S. 113-283, 2014).

Multiple locations

Definition

- This information is reassembled in databases (Gates, 2011) in places like law enforcement facilities, financial centers, Amazon or Netflix facilities, or at Google.

Coding Rules

- Indication of where information is reassembled

Examples

Locations

1. Once the investigator completes his or her work, OPM reviews the results package for completeness (and, when efforts to complete items were unsuccessful, reporting those efforts) and delivers it to the customer agency. The delivery is generally accomplished by electronic means to support electronic adjudication processes in place at Federal agencies" (*The Insider Threat*, 2013, p. 9).
2. "the adjudicating agency only gets a summary of the information that has been gathered during the background investigation. What entity does the actual packaging of the summary that is in turn submitted to the adjudicating agency?" (*The Insider Threat*, 2013, p. 47).
3. Regarding neighborhood checks for TS clearances, "particularly in this area people move and there may not be anybody who knew the subject of the investigation who is available, so we have given guidance to the DOD consolidated adjudication facility, which identifies the types of information which may not be available and which would still allow the DOD CAF to do their adjudication" (*DC Navy Yard Shooting*, 2014, p. 66).
4. The Personnel Investigations Processing System (PIPS)" is OPM's primary fieldwork scheduling and management software" (H. Rep., 2014, p. 13).
5. "OPM plans to implement a system that allows for digital images of any hard copy records obtained during an investigation to be uploaded into the OPM system for review by other investigators" (H. Rep., 2014, p. 23).
6. "One of the main challenges in creating this system is how to pull records from other state and local databases around the country to update the OPM database in near-real time" (H. Rep., 2014, p. 36).
7. "legislation requires OPM to consult with the DNI as well as OPM's top two customers—the Department of Defense and Department of Homeland Security—when creating the database" (H. Rep., 2014, p. 36).

APPENDIX H

SURVEILLERS (ABRIDGED)

- Different surveillant agents
    - Contractors - 88
    - Employees - 35

Sample Passages
Category - Surveillers
Different surveillant agents **Definition** • "Old lines [of control] become blurred – lines that once distinguished police work from private security, or law enforcement from consumer management" (Lyon, 2007, p. 107)
Coding Rules • Indication of multiple actors gathering surveillance
Examples
Contractors 1. "during the Clinton administration, the decision was made to move large amounts of the background investigations work performed by OPM to a contractor workforce" (*The Insider Threat*, 2013, p. 10). 2. USIS holds two contracts with OPM: (1) a Fieldwork Contract to perform investigative fieldwork and (2) a Support Contract to perform support services. Multiple companies hold Fieldwork Contracts with OPM" (*DC Navy Yard Shooting*, 2014, p. 23). 3. KeyPoint provides background investigations to OPM and other government agencies, and "Today, KeyPoint performs approximately 25 percent of the fieldwork conducted by contractors for OPM's background investigations" (*DC Navy Yard Shooting*, 2014, p. 28). 4. CACI is one of the three contractors currently assisting OPM by conducting fieldwork for security clearance investigations" (*DC Navy Yard Shooting*, 2014, p. 36). 5. ESOP created USIS, and according to Mr. Mica, he "was in Congress, actually chaired civil service when we created the initial ESOP. We gave the Federal employees the right to run that initial company, which evolved into Mr. Phillips's company" (*DC Navy Yard Shooting*, 2014, p. 51). 6. "We now have three companies, private companies, that do 70 percent of the work" (*DC Navy Yard Shooting*, 2014, p. 51). 7. Impossible for OPM to do all the work itself (*DC Navy Yard Shooting*, 2014, p. 51). 8. "Ms. ARCHULETA. As I mentioned earlier, sir, the enormity or the large numbers of clearances requested and background investigations that are conducted by OPM is a very large number, and I don't think that right now there is the numbers with Federal employees within FIS to conduct those, that is why we rely on contractors to assist us" (*DC Navy Yard Shooting*, 2014, p. 65). 9. "Ms. ARCHULETA. I believe that with strong quality performance standards that we could rely on contractors to help us" (*DC Navy Yard Shooting*, 2014, p. 65). 10. "Ms. SPEIER. Thank you, Mr. Chairman. Reclaiming my time. I am also concerned that we are wimps in the Federal Government, that even when we are taken to the cleaners by contractors, we go back for more, and that there aren't any penalties that are imposed of any significance. So my question to you, director, is has USIS or Experts been penalized at all?" (*DC Navy Yard Shooting*, 2014, p. 69). 11. Federal workers aren't easily laid off like contractors (*DC Navy Yard Shooting*, 2014, p. 71). 12. "I am of the opinion that Government does best what it checks somebody else doing, and does worse what it does in-house and then tries to hold itself accountable. That has been a problem of Government for a long time, is are we an honest broker of what works and what doesn't" (*DC Navy Yard Shooting*, 2014, p. 77).

13. "We must accept the reality that the most effective security clearance enhancements will focus on improving collaboration between agencies and contactors, since each entity plays a critical role" (*DC Navy Yard Shooting*, 2014, p. 149).
14. “Investigators—often contractors—from Federal Investigative Services within the Office of Personnel and Management (OPM) conduct these investigations for most of the federal government using federal investigative standards and OPM internal guidance as criteria for collecting background information on applicants” (*DC Navy Yard Shooting*, 2014, p. 154).
15. “(10) require that, with respect to any background investigation activities, a Federal employee conducts--”…“(A) any final quality or integrity assurance review conducted by an agency of a background investigation”…“(B) any interview of a covered individual with respect to a background investigation; and” (H.R. 490, 2015)…“(C) any background investigation of a covered individual to determine the person\'s eligibility for a security clearance at the Top Secret level or higher” (H.R. 490, 2015).
16. “Management may not award a contract for--(1) investigative support services to an entity if that entity also has, at the time of award of the contract or at any time during the performance of the contract, another contract in effect with the Federal Government (or with another contractor of the Government at any tier) to provide background investigation fieldwork services; or” (H.R. 490, 2015).
17. “The great majority of background investigations (over 90 percent) are performed by the Federal Investigative Services (FIS) within the Office of Personnel Management (OPM), at the request of other agencies, though several agencies, many of which are in the Intelligence Community, are authorized to conduct their own.” (S. 113-276, 2014).
18. “OPM hires contractors to conduct much of the information collection, and other agencies also use a mix of contractors and federal employees to gather the information needed for a background investigation” (S. 113-276, 2014).
19. “A security clearance is a determination that an individual (whether a federal employee or contractor) is eligible for access to classified national security information. A security clearance may be granted only by a federal agency, and generally only upon completion of a background investigation. Most background investigations are overseen by OPM\'s Federal Investigative Services (actual investigations may be conducted by private investigative firms)” (S. 113-276, 2014).
20. “In FY 2012, OPM prepared over 2.3 million investigative products for federal agencies. Approximately 30 percent of this work was conducted by OPM employees, with the other 70 percent being outsourced to three companies who hold contracts with OPM” (H.Rep., 2014, p. 2).
21. “Committee staff met with representatives of all major stakeholders in the process, including the Office of Personnel Management (OPM), the three contractors performing field investigation services, adjudicators from the Department of Defense (DOD), and private and public companies that employ cleared individuals” (H.Rep., 2014, p. 12).
22. “Three companies hold contracts to perform investigative services on behalf of OPM—U.S. Investigations Services, LLC (USIS), CACI International Inc (CACI), and KeyPoint Government Solutions, Inc. (KeyPoint)” (H.Rep., 2014, p. 14).
23. “We also learned that approximately 75 percent of all the government’s investigations are conducted by contractors, and just one contractor, U.S. Investigations Services (USIS), conducts 65 percent of those investigations” (*Safeguarding Our Nation’s Secrets: Examining the Security Clearance Process*, 2013, p. 3).
24. “Conducting background investigations is one of OPM’s core missions. FIS provides background investigations for over 100 Federal agencies with approximately 10,000 separate submitting offices worldwide. Currently we have more than 2,500 Federal employees and 6,700 contractors that form a nationwide network of field investigators, support staff, as well as a cadre of Federal agents that we have working abroad”

(*Safeguarding Our Nation's Secrets: Examining the Security Clearance Process*, 2013, p. 9).

25. "Our core Federal investigators present us the opportunity to manage highly sensitive and inherently governmental investigation requirements while our contractor workforce permits us to expand and contract operations as the workload and locations dictate" (*Safeguarding Our Nation's Secrets: Examining the Security Clearance Process*, 2013, p. 9).
26. "Mr. MILLER. USIS conducts 45 percent of the overall contract Workload" (*Safeguarding Our Nation's Secrets: Examining the Security Clearance Process*, 2013, p. 13).
27. "I want to get at USIS in terms of not only having the biggest contract to do the background checks; but also having this program support contract. And these contracts are one of my nemeses in my job of overseeing contracts. All through our government there has been an easy way to augment personnel by doing these program support contracts, and at one point in time, and probably still at Homeland Security, you could not tell the contractors from the employees. They were doing the same functions. They were sitting at the same desks. They were working on the same things. One was a contractor and one was not, and partly it was because supposedly they were easier to get rid of" (*Safeguarding Our Nation's Secrets: Examining the Security Clearance Process*, 2013, p. 27).
28. 33 of 999 contract support personnel are federal employees (*Safeguarding Our Nation's Secrets: Examining the Security Clearance Process*, 2013, p. 28).
29. "Also, based on the low-level jobs that they are, it is more financially beneficial for us to have contractors doing that work than bringing on full-time—— (*Safeguarding Our Nation's Secrets: Examining the Security Clearance Process*, 2013, p. 28).
30. McCaskill thinks contractors are more expensive than employees (*Safeguarding Our Nation's Secrets: Examining the Security Clearance Process*, 2013, p. 28).
31. "Mr. MILLER. As we add automation, we are able to downsize the staffing, and so year to year we have seen a decline in the contract staff required for our support services." (*Safeguarding Our Nation's Secrets: Examining the Security Clearance Process*, 2013, p. 28)
32. "It is cost effective to continue using contract support to perform a portion of the background investigation work, with the balance continuing to be performed by federal employees" (*Safeguarding Our Nation's Secrets: Examining the Security Clearance Process*, 2013, p. 60).
33. Using contractors produces a $17.85-million-dollar cost savings as opposed to using Federal equivalents, especially since contractors can easily reduce the number of employees with work load fluxuation (*Safeguarding Our Nation's Secrets: Examining the Security Clearance Process*, 2013, p. 67).
34. Although contract agencies set the workload for contractors, both Federal employees and contractors have the same responsibilities as each other (*Safeguarding Our Nation's Secrets: Examining the Security Clearance Process*, 2013, p. 88).
35. OPM doesn't keep track of the contractor workforce and leaves it to the agencies to maintain staffing. OPM can't say how contractors would translate into FTE's (*Safeguarding Our Nation's Secrets: Examining the Security Clearance Process*, 2013, p. 88).
36. "Often the government employs contractors to compile the information required for the background checks. Final quality reviews of the contractor\'s work product ensure that the background investigation is complete and meets all applicable standards" (S. 113-257, 2014).
37. "S. 2061 would prohibit agencies, when they employ a contractor to perform background investigations, from hiring the same contractor to perform the final quality review of the contractor\'s own work" (S. 113-257, 2014).

38. “This simple rule will prevent a conflict of interest that may otherwise undermine the impartiality and objectivity of the quality review, or give a contractor an unfair competitive advantage over other contractors.” (S. 113-257, 2014).
39. “The federal government relies heavily on contractors to assist with the process of background investigations” (S. 113-257, 2014).
40. “Final decisions based on records compiled by contractors, though, rest with the federal government. For example, the final decision of whether to grant a security clearance must be made by federal employees and rests with the agency that performed the background investigation, or requested that the background investigation be performed, for a particular individual” (S. 113-257, 2014).
41. “Twenty-two agencies (many within the intelligence community) are authorized to perform background investigations, and these agencies may have background checks performed by their own employees or a contractor” (S. 113-257, 2014).
42. “The vast majority of background investigations (over 90 percent) are performed by the Federal Investigative Services (FIS) within the Office of Personnel Management (OPM), at the request of other agencies” (S. 113-257, 2014).
43. “OPM hires contractors to perform investigative services for a majority of the investigations it conducts” (S. 113-257, 2014).
44. “A company called United States Investigations Services, LLC (USIS) has, until very recently, performed almost half of the investigative work contracted out by OPM, and has also provided similar investigative services to several other agencies” (S. 113-257, 2014).
45. “One issue raised by Committee members was the appropriate role of contractors in conducting background investigations, and whether contractors ever conduct the final quality reviews of their own work” (S. 113-257, 2014).
46. “This concern was heightened by the announcement of the fraud allegations against USIS, and the fact that USIS conducted security clearance Background investigations for both Navy Yard shooter Aaron Alexis and former National Security Agency contractor employee Edward Snowden” (S. 113-257, 2014).
47. “In a letter to Ranking Member Coburn following up on her testimony, OPM Acting Director Elaine Kaplan explained that some lower-level investigations may be reviewed by contract employees, rather than federal employees” (S. 113-257, 2014).
48. “OPM reversed its policy on February 6, 2014, when OPM Director Katherine Archuleta announced that only federal employees would conduct the final quality review before an investigative product is sent by OPM to the agency that requested the review” (S. 113-257, 2014).
49. “This decision, though, is an administrative one and does not preclude a future OPM Director from again allowing contractors to review their own work. Nor does this decision preclude other agencies from permitting contractors to conduct the final quality reviews of their own work” (S. 113-257, 2014).
50. “The bill [S. 2061] in no way discourages a contractor performing background investigations from conducting internal quality reviews to ensure that the product meets requisite standards before the product is presented to OPM (or to any other agency that hired the contractor). However, the bill will ensure that the final quality review is not performed by the same contractor” (S. 113-257, 2014). The committee unanimously adopted the substitute bill.
51. “We have a multisector workforce, comprised of military, civilian, and contractor personnel. We have worked to ensure that robust vetting policies and processes are applied to all individuals with access to Federal facilities, networks, or classified information in a consistent manner” (*The Navy Yard Tragedy,* 2013, p. 8).
52. “the need to protect our national security is no less critical when the work is performed by contractors than when it is performed by Federal employees; second, the men and women who make up the contractor workforce are no less patriotic than their government counterparts, and in fact, many have had meaningful careers as Federal employees or in the Armed Forces” (*The Navy Yard Tragedy,* 2013, p. 8).

53. “Investigators, often contractors for OPM, conduct these investigations for most of the government” (*The Navy Yard Tragedy,* 2013, p. 15).
54. “the contractors have an obligation under the contract to conduct their own quality reviews of investigations. Once they finish their quality reviews, they send the product to OPM, and we conduct our own quality reviews of the investigation” (*The Navy Yard Tragedy,* 2013, p. 18).
55. “we have done a number of things as soon as we became aware of the allegations. With respect to OPM, we have significantly increased the number of government personnel performing contractor oversight by increasing the number of people, the full-time equivalent (FTE) levels, and realigning our internal staff” (*The Navy Yard Tragedy,* 2013, p. 19).
56. “I think this is a misimpression that a lot of folks have—that the contractors are doing both the investigations and the adjudications, and that would be a really bad system. But, in fact, the adjudication is not done by the contractors. It is done by the agency that is granting the clearance…Senator COBURN. Can they use a contractor to do it? Ms. KAPLAN. No. That is an inherently governmental function. It is not something we would entrust to a contractor” (*The Navy Yard Tragedy,* 2013, p. 21).
57. “Senator COBURN. Let me ask you another question. We are using contractors for this clearance process. To me it would seem that the clearance process in and of itself is an inherently government function, not just the adjudication but the investigation…Mr. JORDAN. Senator, the collection of information, the analysis is not an inherently governmental function. As Director Kaplan said, the decision, the adjudication is an inherently governmental function. That should only be performed by government employees. But the collection of information is not inherently governmental.” (*The Navy Yard Tragedy,* 2013, p. 21).
58. “What we have done—and it is not just oversight of USIS, because we have other contractors and we have Federal employees, quite frankly, who do the work, too. They need to be watched” (*The Navy Yard Tragedy,* 2013, p. 24).
59. “contractors perform background investigations, and, yes, contractors can perform quality reviews on those investigations. But only government employees make a determination as to whether to grant a security clearance to someone” (*The Navy Yard Tragedy,* 2013, p. 38).
60. “The companies that are doing the investigations have an obligation under the contract to also do a quality review. But then we do another quality review, and the purpose of their quality review is we would like them to catch errors before the file gets to us, but we do a quality review as well. Senator COBURN. So OPM is the final validator of the completeness of the investigation? Ms. KAPLAN. To some extent. I mean, I think another thing that validates the completeness of the investigation, it gets sent to an adjudicator. An adjudicator may want more information. And so ultimately it is a collaborative effort. They may send something back to us. But we are the arbiter of whether we have provided an adequate investigative product, a quality investigative product” (*The Navy Yard Tragedy,* 2013, p. 38).
61. Every investigation is validated Federally by OPM (*The Navy Yard Tragedy,* 2013, pp. 38-9).
62. The Clinton administration decided to move a chunk of OPM’s work to contractors (*The Navy Yard Tragedy,* 2013, p. 58).
63. "The process for contractors and federal employees is exactly the same for the same level of clearance sought", and whether an individual needs a clearance and at what level are always made by a Federal employee (*The Navy Yard Tragedy,* 2013, p. 97).
64. Adjudications are also only made by Federal employees (*The Navy Yard Tragedy,* 2013, p. 98).
65. Only 30% of investigations are conducted by OPM or DSS federal employees (*The Navy Yard Tragedy,* 2013, p. 98).

66. While there are allegations of wrong-doing, "60 percent of known cases of impropriety involve in-house federal civilian government employees" (*The Navy Yard Tragedy,* 2013, p. 98).
67. Although adjudicating is an inherently Federal function, conducting background investigations is not (*The Navy Yard Tragedy,* 2013, p. 121).
68. OPM contracts cover "1) Receipt, screening, data entry, case file maintenance 2) conducting investigative fieldwork 3) case reviewing/closing, and 4) post-closing support" (*The Navy Yard Tragedy,* 2013, p. 121).
69. All of these are carried out as per the Federal investigative standards and the Investigator's Handbook given to fieldwork investigators (*The Navy Yard Tragedy,* 2013, p. 121).
70. Regarding more armed guards that can respond to active shooter scenarios, "Now, there is a possibility that we could possibly deputize some of our contractor personnel. However, that would clearly be more costly, and we would have to figure out how we would do that" (*The Navy Yard Tragedy,* 2013, p. 155).
71. Regarding the guards doing the physical security at buildings, "And then you audit whether or not they are telling you the truth rather than spend a whole bunch of money, us running all 13,000 people when they are really not our employees. They are contract employees for somebody that took a contract to guard a building" (*The Navy Yard Tragedy,* 2013, pp. 164-5).
72. Regarding the use of contractor for FIS, Archuleta feels that the employee v. contractor ratio relies on workload, resource needs, and having the ability to expand and contract as required to meet varying demands for investigative products, and the balance should be the most cost-effective combination (Nomination of Hon. Katherine Archuleta, 2013, p. 81).
73. OPM will review if it is cheaper to hire contractors or government employees for program support (currently, only 35 of 999 are government employees) (Nomination of Hon. Katherine Archuleta, 2013, p. 105).
74. "Additionally, Executive Orders 12968 and 10865 do not require a uniform government-wide process, and in fact establish two parallel processes, one for contractors and one for government employees" (USGAO, 2014b, p. 40)
75. "Federal agencies rely extensively on contractors to provide IT services and operate systems to help carry out their missions. For example, we reported that in fiscal year 2012, the Department of Defense obligated approximately $360 billion for contracts for goods and services, such as information technology and weapon systems maintenance" (USGAO, 2014a, p. 4).
76. "The ability to contract for technology services can allow an agency to obtain or offer enhanced services without the cost of owning the required technology or maintaining the human capital required to deploy and operate it" (USGAO, 2014a, p. 4).
77. "Specifically, contractors and their employees provide services and systems to agencies at agency and contractor facilities, directly and by remote access. Services can include computer and telecommunication systems and services, and testing, quality control, installation, and operation of computer equipment" (USGAO, 2014a, pp. 4-5).
78. OMB "defines five primary categories of contractor relationships associated with securing systems and information: (1) service providers; (2) contractor support; (3) government-owned, contractor-operated facilities; (4) laboratories and research centers; and (5) management and operating contracts. Table 1 describes the five types of contractual relations identified by OMB" (USGAO, 2014a, p. 5).
79. "In fiscal year 2012, OMB reported that contractor employees accounted for 33 percent of all IT security personnel at the 24 Chief Financial Officers Act agencies." (USGAO, 2014a, p. 5).
80. Chart of # of contract IT providers (USGAO, 2014a, p. 6).

81. “DOE, DOT, EPA, OPM and State officials were unable to demonstrate that contractor employees had received the necessary training despite assessment results that stated they had” (USGAO, 2014a, p. 17).
82. “Nevertheless, the inconsistent implementation of OMB’s reporting guidance by agencies in reporting the number of contractor-operated systems demonstrates that existing outreach and education efforts during face-to-face meetings with agency information security officials are not always resulting in accurate reporting of agencies’ reliance on contractors to operate systems and process government information on their behalf” (USGAO, 2014a, p. 23).
83. “The Office of Personnel Management (OPM) conducts the great majority of the investigations, though several agencies, many of which are in the Intelligence Community, are authorized to conduct their own” (S. 113-283, 2014).
84. “OPM hires contractors to conduct much of the information collection, and other agencies also use a mix of contractors and federal employees to gather the information needed for a background investigation” (S. 113-283, 2014).
85. “Having private guards can increase the accountability for the taxpayer, but DHS cannot be deficient in its management responsibilities and must deploy the right number of guards, based on risk” (*Facility Protection*, 2013, p. 2).
86. “I also hope that we will be able to explore the true cost of contracting services, using contractors versus dedicated civil servants or professionals who are in those jobs for their careers. There is a balance that we have to strike in terms of cost savings and efficiencies versus some level of dependability and building a culture that might, in fact, ultimately prevent these kinds of activities in the future” (*Facility Protection*, 2013, p. 5).
87. “My legislation seeks to move FPS away from its over-reliance on contract security guards, and to instead build up the agency’s internal capacity” (*Facility Protection*, 2013, p. 6).
88. “Yes, the Department does contract with private firms to conduct background checks. The Office of Personnel Management and the Department of Defense have oversight responsibility for the background investigation contract workforce. OPM delegates investigative authority to certain DHS components, who then employ contract background investigators. It is a requirement of the delegation that contract investigators must have been appropriately adjudicated. The Department of Defense has responsibilities regarding the security clearance adjudications of contract employees under the National Industrial Security Program. DHS accepts reciprocity of the investigation and adjudication of contract background investigators” (*Facility Protection*, 2013, p. 55).

Employees

1. S. 2683 – the CORRECT Act recommends: 6. “Appeal to the Merit Systems Protection Board “An employee for whom a final determination of ineligibility for a national security position has been made is entitled to appeal to the Merit Systems Protection Board” (S. 2683, 2014).
2. S. 2683 – the CORRECT Act recommends: 8. “Report on media contacts policy for intelligence personnel –‘describe how each such element\'s implementation of such directives protects the free speech rights of intelligence community personnel, including intelligence community personnel who choose to discuss unclassified public policy issues with friends or family members who may use new media technologies’” (S. 2683, 2014).
3. When Federal employees are suspected of falsification, they are placed on administrative leave until the case is resolved and evidence is gathered to support being fired, while still getting paid. Contractors are immediately removed from contracts. Archuleta believes agencies need to hold employees engaging in misconduct accountable, but it is also important to give these employees due process (Nomination of Hon. Katherine Archuleta, 2013, p. 81).
4. “Specifically, DHS and DOD have implemented the requirements for the revocation process contained in Executive Orders 12968 and 10865 in different ways for different

groups of personnel. Although certain differences are permitted or required by the executive orders, GAO found that implementation by some components could potentially be inconsistent with the executive orders in two areas. As a result, some employees may not be provided with certain information upon which a revocation appeal determination is based, and may not be told that they have a right to counsel" (USGAO, 2014b, p. intro).

5. "Inconsistent implementation of the requirements…have resulted in employees in some agency components and workforces experiencing different protections and processes than employees in other agency components and workforces" (USGAO, 2014b, p. 23).
6. "one DHS component—the Coast Guard—was not notifying its military personnel of their right to be represented by counsel or other representative at their own expense, but rather was erroneously informing military personnel that they had no right to counsel" (USGAO, 2014b, p. 34).
7. "DHS and DOD employees whose eligibility to access classified information has been revoked may not have consistent employment outcomes, such as reassignment or termination, because these outcomes are generally dependent on several factors, including the agency's mission and needs and the manager's discretion" (USGAO, 2014b, p. 41).
8. "Communication between personnel security and human capital offices at DHS and DOD varies, but lack of communication between these offices could result in adverse employment actions being taken prematurely or in inappropriate use of personnel security or human capital processes" (USGAO, 2014b, p. 44)**.**
9. "A lack of communication between the human capital and personnel security offices could result in adverse employment actions being taken prematurely or in the inappropriate use of personnel security processes in lieu of human capital processes" (USGAO, 2014b, p. 46).
10. "Ordinarily, most federal civilian employees have a right to appeal serious adverse employment actions taken against them to the Merit Systems Protections Board. However, in the security clearance context, federal case law [see Navy v. Egan, 484 U.S. 518 (1988), and Kaplan v. Conyers, 733] has limited the scope of the board's review of adverse actions. Specifically, the board may review appeals of adverse employment actions resulting from a denial or revocation of a security clearance or a determination that an employee is not eligible to hold a sensitive position for specific procedural issues, but the board cannot review the substance of a security clearance denial or revocation, or a finding that an employee is not eligible to hold a sensitive position" (USGAO, 2014b, p. 47).
11. "To help ensure that all employees within DHS receive the same protections during their personal appearance, we recommend that the Secretary of Homeland Security direct the Chief Security Officer to revise and finalize the DHS instruction regarding the personnel security program to clarify whether or not employees are allowed to cross-examine witnesses during personal appearances" (USGAO, 2014b, p. 55).
12. "To help ensure that all employees within DOD receive the same rights during the revocation process, we recommend that the Secretary of Defense • direct the Secretary of the Navy to revise Secretary of the Navy Manual M-5510.30 to specify that any information collected by the Navy PSAB from the employee's command will be shared with the employee, who will also be given the opportunity to respond to any such information provided; and • direct the Secretary of the Army to revise Army Regulation 380-67 to specify that any information collected by the Army PSAB from the employee's command or by the Army PSAB itself will be shared with the employee, who will also be given the opportunity to respond to any such information provided" (USGAO, 2014b, p. 56).
13. "To help ensure that all employees are treated fairly and receive the protections established in the executive order, we recommend that the Secretary of Homeland Security direct the Commandant, U.S. Coast Guard, to revise the Coast Guard

instruction for military personnel to specify that military personnel may be represented by counsel or other representatives at their own expense" (USGAO, 2014b, p. 56).

14. "To help ensure that similarly situated individuals are treated consistently, and to facilitate oversight and help ensure the quality of the security clearance revocation process, we recommend that the DNI review whether the existing security clearance revocation process is the most efficient and effective approach. In this review, the DNI should consider whether there should be a single personnel security clearance revocation process used across all executive-branch agencies and workforces, with consideration of areas such as the timing of the personal appearance in the revocation process, and the ability to cross-examine witnesses" (USGAO, 2014b, p. 56).
15. "To facilitate coordination between personnel security and human capital offices regarding how a security clearance revocation should affect an employee's employment status, and to help ensure that individuals are treated in a fair and consistent manner, we recommend that • the Secretary of Homeland Security direct the Under Secretary for Management to review and revise policy regarding coordination between the personnel security and human capital offices to clarify what information can and should be communicated between human capital and personnel security officials at specified decision points in the revocation process, and when that information should be communicated; and • the Secretary of Defense direct the Under Secretary of Defense for Personnel and Readiness, in consultation with the Under Secretary of Defense for Intelligence, to review and revise policy regarding coordination between the personnel security and human capital offices to clarify what information can and should be communicated between human capital and personnel security officials at specified decision points in the revocation process, and when that information should be communicated" (USGAO, 2014b, p. 57).
16. Some "have real concerns that the proposed guidance is inadequate and that it could have negative and substantial implications on taxpayers, national security, and Federal employee rights" (*Safeguarding Our Nation's Secrets: Examining the National Security Workforce*, 2013, p. 2).
17. "These concerns are compounded by this summer's Kaplan v. Conyers and Northover decision. This case involved two Federal employees who lost their jobs when their employing agency stripped them of their sensitive position status. Because the Conyers decision denied these employees their rights to due process through the Merit Systems Protection Board (MSPB), there is a real potential that tens of thousands of employees across the Federal Government have just lost their fundamental right to appeal a personnel decision, regardless of what drove that decision" (*Safeguarding Our Nation's Secrets: Examining the National Security Workforce*, 2013, p. 2).
18. Specific Kaplan V. Conyers details. (*Safeguarding Our Nation's Secrets: Examining the National Security Workforce*, 2013, pp. 61-64).
19. In the Kaplan v. Conyers case, "the U.S. Court of Appeals for the Federal Circuit, in a 7–3 decision, held that the Merit Systems Protection Board, lacks jurisdiction to review the merits of executive branch risk determinations regarding eligibility to hold national security sensitive positions… The Federal Circuit based its decision on long-standing precedent, specifically the Supreme Court's 1988 decision in Department of the Navy v. Egan, that the MSPB, in reviewing an appeal of an adverse action cannot review the merits of an agency decision to deny an employee security clearance. The Federal Circuit held that Egan controlled all such national security determinations, not just those related to access to classified information (*Safeguarding Our Nation's Secrets: Examining the National Security Workforce*, 2013, pp. 7-8, 37).
20. "Conyers eliminated the right to a meaningful hearing before the U.S. Merit Systems Protection Board. The proposed regulations exacerbate this problem by allowing agencies to pick and choose which employees will have the right to due process before the MSPB. Conyers and the proposed regulations are only the latest injustices

inflicted upon Federal workers" (*Safeguarding Our Nation's Secrets: Examining the National Security Workforce*, 2013, pp. 10, 61).

21. "The Conyers' ruling rejected the text, the structure, and the history of the Civil Service Reform Act (CSRA), along with the plain language of Egan to hold that the MSPB may not review the merits of an agency determination that an employee is ineligible to hold a sensitive position" (*Safeguarding Our Nation's Secrets: Examining the National Security Workforce*, 2013, pp. 10-11).
22. "In both Conyers and the proposed regulations are allowed to stand, executive branch agencies will have the unreviewable power to deprive hundreds of thousands of employees the protections that Congress gave them in the CSRA. That, Senators, is likely to be an irresistible invitation to abuse" (*Safeguarding Our Nation's Secrets: Examining the National Security Workforce*, 2013, pp. 11, 61).
23. "We are deeply concerned that the national security claims here and throughout the government really threaten to engulf our government and, with cruel irony, will make us less safe. In August of this year, this Court decision in Conyers stripped Federal employees in national security sensitive positions of their right to an appeal an adverse action, setting the stage to also strip due process rights for actions that are discriminatory or in retaliation for whistle blowing" (*Safeguarding Our Nation's Secrets: Examining the National Security Workforce*, 2013, p. 11).
24. "This deeply flawed decision in Kaplan v. Conyers armed agencies with sweeping power that affects untold numbers of civil servants, untold because OPM cannot say exactly how many position holders there are" (*Safeguarding Our Nation's Secrets: Examining the National Security Workforce*, 2013, p. 11).
25. "While there is a need for additional screening for a very limited number of civilian positions with specific national security responsibilities but no access to classified information, extensive background checks should never be a predicate for denying due process rights" (*Safeguarding Our Nation's Secrets: Examining the National Security Workforce*, 2013, p. 12).
26. "Congress gave the Civil Service and whistleblower protections to this critical workforce to foster accountability for waste, fraud, and abuse. These workers had, for years, been able to challenge adverse personnel actions at the Merit Systems Protection Board, but not anymore" (*Safeguarding Our Nation's Secrets: Examining the National Security Workforce*, 2013, p. 12).
27. "We agree, it is about time [for updated policies], but unfortunately, it does nothing to assure us that the Obama Administration plans to curb the practically unlimited discretion afforded to agencies, improved, efficient oversight, or protect critical rights or whistleblowers and Civil Service" (*Safeguarding Our Nation's Secrets: Examining the National Security Workforce*, 2013, p. 12).
28. "what we could do here to make sure that the rules that ODNI and OPM are putting in place actually do what I think you guys want them to do; and yet, does not break the bank, protects due process of workers" (*Safeguarding Our Nation's Secrets: Examining the National Security Workforce*, 2013, p. 23).
29. "Congress is going to have to fix the law and make sure that these civil servants and whistleblowers have access to review at the Merit Systems Protection Board" (*Safeguarding Our Nation's Secrets: Examining the National Security Workforce*, 2013, p. 24).
30. These changes are amplified by Conyers which can essentially be used to say every employee is sensitive and has no MSPB rights which goes against CSRA (*Safeguarding Our Nation's Secrets: Examining the National Security Workforce*, 2013, p. 64).
31. Kaplan v. Conyers ruled that MSPB "could not engage in substantive review of Department of Defense (DoD) decisions concerning the eligibility of employees to occupy "sensitive" positions, even though the MSPB has been capably doing so for decades" (*Safeguarding Our Nation's Secrets: Examining the National Security Workforce*, 2013, p. 77).

32. Conyers give agencies incentives to have more positions as "sensitive" so that there can be no review if fired. This is problematic because, for example, at CBP, almost all the 24,000 bargaining unit positions are designated as noncritical-sensitive but only a fraction need clearances (*Safeguarding Our Nation's Secrets: Examining the National Security Workforce*, 2013, p. 77).
33. Ineligibility can be "based on incomplete or faulty background information; it can be for reasons motivated by an employee's race religion, or constitutionally protected speech; it can be for retaliatory reasons; it can be because the employees is a whistleblower" and the designation of ineligibility can't be reviewed due to Conyers (*Safeguarding Our Nation's Secrets: Examining the National Security Workforce*, 2013, p. 77).
34. "By eliminating the Board from the equation, employees will have no forum in which to obtain independent, meaningful review of agency actions arising from the denial or loss of eligibility to occupy a sensitive position or the denial or loss of a security clearance" (*Safeguarding Our Nation's Secrets: Examining the National Security Workforce*, 2013, p. 282).
35. In order to make sure security clearance position designations don't get overused to be a barrier to entry for diverse candidates, "Conyers should be overruled. Full merits review should be restored to the Board. Second, agency position designation determinations should be subject to ongoing and neutral civilian oversight...Employees are often in the best position to say what the actual duties of a position are and it is those duties that should guide the designation process." Problems with over and under designation could be addressed by having an oversight system which allows employees to have a voice in the system (*Safeguarding Our Nation's Secrets: Examining the National Security Workforce*, 2013, p. 283).

APPENDIX I

TECHNOLOGY (ABRIDGED)

BIs using tech

- Accuracy 1
- Automation 35
- Collection 1
- Continuous evaluation 14
- Control 1
- Cost 3
- Database 47
- Delivery 1
- Duplication 7
- Enterprise-wide /database 11
- Exclusion 1
- Internet/social media 18
- Paper 2
- Programs 24
- Reliability 17
- Sharing 17
- Solution 3
- Tools 10
- Unrealistic 19
- Web-based 4

Tech and biometrics

- Automation 1
- Continuous evaluation 1
- Database 1
- Enterprise 1
- Fingerprints 4
- Program 1

Confinement and exclusion

- Keeping in / keep out 7

Everyday use of tech

- Public and social media 31

Sample Passages

Category – Technology

BIs using tech

Definition

- "Codes, usually processed by computers, sort out transactions, interactions, visits, calls, and other activities" (Lyon, 2003, p. 13)
- Technology reconstitutes the body from the observable into code (Zureik, 2003, p. 40) "A key trend of today's surveillance is the use of the searchable **database** to process personal data for various purposes" (Lyon, 2003, p. 14)

Coding Rules

- Evidence of technological involvement in BIs
- Use of technology in BIs
- Names of tech programs to track individuals
- Databases

Examples

Accuracy

1. "(8) increase the use of digitally processed fingerprints as a substitute for ink or paper prints to reduce error rates and improve portability of data" (H.R. 490, 2015).

Automation

1. "Manual checks are inefficient and resource-intensive" (*The Insider Threat*, 2013, p. 16).
2. "C.E., as envisioned in the reformed security clearance process, includes automated record checks of commercial databases, Government databases, and other information lawfully available" (*The Insider Threat*, 2013, p. 16).
3. I want to come "up with a solution to give you guys the tools that you need to help keep our Country safe and make this process much more streamlined, much more automated, and much more responsive to the needs so we avoid another tragedy like Navy Yard" (*DC Navy Yard Shooting*, 2014, p. 61).
4. "Mr. FARENTHOLD. It seems like that is something that could, at a very simple level, be automated. You have their name, you have their date of birth, you have their social security number. Okay, after Healthcare.gov, I am questionable about the Government's ability to automate anything or compute its way out of a paper bag, but that seems like a relatively trivial" (*DC Navy Yard Shooting*, 2014, p. 61)
5. The Security Clearance and Reform act of 2014 must lay out ways to streamline and eliminate outdated manual processes "in favor of electronic and accessible investigative databases"" (*DC Navy Yard Shooting*, 2014, p. 148).
6. "(6) enhance methods for reducing or eliminating manual processes with respect to security clearance background investigations, and automating and integrating the elements of such investigations and adjudication processes, including—"(A) the security clearance application process; " "(B) field investigator reporting; (C) investigation case management; (D) the collection, analysis, storage, retrieval, and transfer of data and records; "(E) the submission of any background investigation report to an agency for adjudication; and (F) records management for security clearance adjudication determinations" (H.R. 490, 2015).
7. "(7) reduce or eliminate the use of databases and information sources that cannot be accessed and processed electronically, or modify such databases and information sources to enable electronic access and processing" (H.R. 490, 2015).
8. "The United States issues approximately 5 million clearances to government employees and contractors, and the ongoing review process is conducted manually, by a limited number of investigators. Further, the manual process is flawed" (Enhanced Security, 2013).
9. "The government needs to utilize existing solutions, which are already used by law enforcement, to automate random audits on individuals with active security clearances" (Enhanced Security, 2013).

10. “The Department of the Treasury’s Offset Program (TOP), or a similar mechanism, may provide an opportunity for federal agencies to perform an automated check of both security-clearance applicants and current clearance holders to determine whether they have unpaid federal debts that would include tax debts, while not violating IRS section 6103 requirements. TOP is an automated process administered by the Department of the Treasury in which certain federal payments, such as contractor and federal salary payments, are reduced to collect certain delinquent tax and nontax debts owed to federal agencies, including the IRS (USGAO, 2013, pp. 22-3).
11. “OPM then officially opens the investigation and begins scheduling all necessary work to field personnel. PIPS performs some scheduling automatically” (H. Rep., 2014, p. 13).
12. “USIS contract employees working on the support services contract manually schedule other parts of the field work” (H. Rep., 2014, p. 13).
13. Automated agency checks occur online and as per Miller, “There was a process we call consolidated leads. So when we could obtain a record in an automated way, reaching out to a statewide system or an agency system to actually obtain the information, we centralized that process. So if an investigation requires certain leads that can be done in an automated way we have folks that do the consolidated leads. They reach out, obtain it in an online fashion, update our record system, PIPS, with the results of that search, and it becomes part of the investigation” (H. Rep., 2014, p. 14).
14. “If it's a secret investigation where most of the checks are automated, there is no interviews associated with it” (H. Rep., 2014, p. 21).
15. the auto release function, to the best of my [knowledge], is auto releases to review, because there are certain timeliness mandates that we have in the system. There is a function in the system that when a contractor or a Fed finishes an investigation, that the system notices, okay, all the items are there, all the ROIs are there. It gives the contractor on their side a certain time period to conduct their initial quality review before they provide it to the Federal staff for our quality review. If they exceed that time period, the system is scheduled to automatically release it to full Fed review. My understanding, it was put in the system, one, to keep the cases moving and to not allow a backlog in review, contract review side of the house” (H. Rep., 2014, p. 25), and it is essential to the process because “Timeliness. It is all based on making sure we meet the timeliness mandates of 40 days” (H. Rep., 2014, p. 26).
16. “Cases that involved only automated records checks and have no leads sent to the field, include Secret-level NACLC or NAC investigations” (H. Rep., 2014, p. 27).
17. “[A] new investigation product in FY 2011 that provides for a validated suite of automated records checks that can be used as an annual assessment of individuals cleared at the Top Secret level” (H. Rep., 2014, p. 33).
18. “The processes supporting these investigative activities are highly integrated, automated, consistently measured against timeliness and quality performance standards for Federal hiring and security clearance process reforms” (*Safeguarding Our Nation’s Secrets: Examining the Security Clearance Process*, 2013, p. 9).
19. “Mr. MILLER. As we add automation, we are able to downsize the staffing, and so year to year we have seen a decline in the contract staff required for our support services.” (*Safeguarding Our Nation’s Secrets: Examining the Security Clearance Process*, 2013, p. 28).
20. OPM's automated field investigator tools in the Field Work System (FWS) (*Safeguarding Our Nation’s Secrets: Examining the Security Clearance Process*, 2013, p. 70).
21. OPM "has assumed responsibility for validating the reliability of public information from state and local repositories as they evolve to automate law enforcement, birth citizenship and court records." (*Safeguarding Our Nation’s Secrets: Examining the Security Clearance Process*, 2013, p. 70).
22. “Although OPM processes are largely automated, OPM relies on contractor support to convert records received in a myriad of configurations and forms from thousands of

information providers into automated information that will support efficient adjudicative processing. Until the largest government records repositories can be reformed to provide fully automated data exchanges, OPM will have to continue to rely on manpower intensive contract support to convert the information received into automated information that can be incorporated into e-Deliverable background investigation products" (*Safeguarding Our Nation's Secrets: Examining the Security Clearance Process*, 2013, p. 89).

23. Automation allows for more timely processing of investigative requests which makes other agencies more efficient and able to hire people faster (*Safeguarding Our Nation's Secrets: Examining the Security Clearance Process*, 2013, p. 89).
24. "FIS is to begin testing a function that will allow OPM to collect birth certification data directly from state data repositories via automated linkage (*Safeguarding Our Nation's Secrets: Examining the Security Clearance Process*, 2013, p. 90).
25. "CE, as envisioned in the reformed security clearance process, includes automated record checks of commercial databases, government databases, and other lawfully available information" (*The Navy Yard Tragedy*, 2013, p. 12).
26. "As I understand your testimony, you have talked about this idea in your testimony of automated record checks, yet you say there is more research required. I do not understand how, if we do not have some random checks and we are relying totally on self-reporting— frankly, people's lives change dramatically and can change in 5 years' time—that we will have a system that really verifies that people should maintain their clearance status" (*The Navy Yard Tragedy*, 2013, p. 28) .
27. "A number of pilot studies have been initiated to assess the feasibility of select automated records checks and the utility of publicly available electronic information, to include social media sites, in the personnel security process... More research is required to assess resource impacts and determine the most effective method to utilize publically available electronic information while protecting the privacy and civil liberties of those individuals being evaluated" (*The Navy Yard Tragedy*, 2013, p. 65).
28. Automation in BIs includes electronic case management systems, adjudication tracking systems, continuous evaluations technologies, eQIP and eAdjudication (*The Navy Yard Tragedy*, 2013, p. 112).
29. "The use of automated searches and social media enhance an adjudication's ability to make a well information eligibly determination" (*The Navy Yard Tragedy*, 2013, p. 126).
30. "continuous evaluation of employees and contractors who are eligible for access to classified information, which involves automated data checks from sources such as credit checks, social media, and personnel records" (USGAO, 2014b, p. 2).
31. CE "involves automated data checks from sources such as credit checks, social media, and personnel records to provide near-real-time notification of relevant information to help identify potential risks to national security" (USGAO, 2014b, p. 2).
32. "continuous evaluation of employees and contractors who are eligible for access to classified information, which involves automated data checks from sources such as credit checks, social media, and personnel records" (USGAO, 2014b, p. 2).
33. "Positions is now available to most applicants, and investigators and/or adjudicators have increased access to electronic record repositories and electronically transmitted background investigations. In addition, automated national security adjudication business rules allow for automated determinations for favorable Secret investigations for many departments and agencies" (*Safeguarding Our Nation's Secrets: Examining the Security Clearance Process*, 2013, p. 83).
34. "witnesses reported that all government agencies already conduct some automated electronic record checks now, and described the Automated Continuous Evaluation System (ACES) being developed by DoD to test, on a large population of cleared military, civilian, and contractor personnel, the concepts of conducting one-time inquiries and then moving towards providing real-time updates as soon as an arrest is posted on a law- enforcement database, for example, or when other relevant information becomes available" (S. 113-283, 2014).

35. “identify high risk populations through the use of automated records checks (e.g., derogatory credit or criminal activity)” (S. 113-283, 2014).

APPENDIX J

OVERALL PROCESS (ABRIDGED)

Overall Process- 529

- Communication (lack) - 34
  - Definition: There is not enough communication between BI stakeholders.
  - Rules: Passages discussing that more communication is needed at any step of the process.
    - Adjudications - 4
    - Agencies – 17
    - Contractor/employees (non-investigators) - 3
    - Investigators – 5
    - Law enforcement - 3
    - Databases - 2
- Finances - 37
  - Definition: The costs of the investigative process can cause problems.
  - Rules: Passages advocating for increasing funds were included.
    - Inspector General - 12
    - Designations -15
    - Monitoring - 5
    - OPM - 2
    - Timeliness - 3

- General questions - 26
  - Definition: Miscellaneous questions posed about the BI.
  - Rules: Questions addressing the BI process were included.
    - Questions - 26

- Historical precedence – events - 140
  - Definition: Events show the BI is flawed, and processes need to change in light of specific events.
  - Rules: Events used to show that there are problems in the BI process were included in this section.
    - 9/11 - 21
    - Alexis - 56
    - Elder - 3
    - Generic recent events - 10
    - Hasan – 4
    - Holocaust Museum - 1
    - Manning – 10
    - Oklahoma City - 4
    - Snowden – 29
    - Wheeling, WV 2

- Historical precedence-studies - 44
  - Definition: Studies questioning the BI process have long existed, even before Snowden.
  - Rules: Included were passages mentioning past reports analyzing the BI.
    - Continuous evaluation - 2
    - Legislation-past work - 24
    - Outdated - 4
    - Quality - 2
    - Reports - 8
    - Timeliness - 4

- Legislation-current - 30
  - Definition: Legislation is inadequate in scope and needs to be amended.
  - Rules: Passages discussing legislation about the BI were included.

        - Defense Authorization Bill - 1
        - General - 3
        - H.R.2860 - 1
        - H.R. 4022 - 2
        - S. 1276 – 5
        - S. 1618 - 3
        - S. 1744 - 10
        - S. 2061 - 4
        - S. 2683 - 1
        - Taxes - 1
- Prediction - 27
    - Definition: There should be more prediction of events.
    - Rules: Passages discussing prediction were included.
        - Better processes - 3
        - High risk - 7
        - Legislation - 1
        - Red flags - 13
        - Predictive metrics - 2
        - Timely information - 1
- Process - 76
    - Definition: There was criticism of the whole process and not necessarily faulting one element of the procedure.
    - Rules: Passages discussing the BI process as troubled or problematic were included.
        - Consequences of bad BIs - 28
        - Costly - 2
        - Currently broken - 27
        - Need new processes - 19
        - No way to standardize - 1
- Self-reporting - 24
    - Definition: The self-reporting function of BIs is flawed.
    - Rules: Discussions of self-reporting were included.
        - Examples of self-reporting problems - 4
        - Need CE and not self-reporting - 5
        - Vulnerability - 13
        - What is needed - 2
- Speed, efficiency, timeliness - 34
    - Definition: Timeliness is an issue whether it is too fast or too slow.
    - Rules: Passages discussing the speed of the investigations were included.
        - Cause bad behavior - 12
        - Examples of why we need - 5
        - General goal of reform - 6
        - ME delays - 1
        - Requesting more information delays - 2
        - Requirements - 5
        - Tax delays - 1
        - Tech - 2
- Technology - 56
    - Definition: Technology is helping, should help more, and remains a source of vulnerability.
    - Rules: Passages discussing technology or specific programs were included.
        - Databases - 7
        - Need more tech - 15
        - Problems with tech - 34

Communication, lack of

Adjudications

1. “Legislation could also finally allow agency adjudicators to directly speak with OPM investigators, giving adjudicators additional information on an applicant when deciding whether or not to grant a clearance” (H. Rep., 2014, p. 3).
2. “this information on Alexis’ mental state did not get to Department adjudicators, who could have taken steps to suspend or terminate his security clearance” (H. Rep., 2014, p. 11).
3. Regarding the use of the Internet, “Unfortunately, investigators conducting federal security clearance background checks do not see, search, or receive reports of the vast amount of information available online. Nor do current federal security process guidelines allow the adjudicators who grant the clearances to access this information” (H. Rep., 2014, p. 36).
4. “Currently, agency adjudicators do not speak with the OPM or contract investigators who investigated a security clearance application… Adjudicators cannot simply contact investigators to ask follow-up questions about the file. The ability to do so would be extremely helpful to adjudicators in certain instances.” (H. Rep., 2014, p. 38).

Agencies

1. “Also, based on the level of reinvestigation and records collected, security offices are not always provided relevant information on individuals of incidents occurring in their employment” (*The Insider Threat*, 2013, p. 48).
2. “Congress, OPM, the Department of Defense (DOD) and other federal agencies must work together to tighten this process and ensure that fewer individuals like Aaron Alexis slip through the cracks in the future” (H. Rep., 2014, p. 3).
3. “Since Alexis was not ultimately charged with unlawfully discharging a firearm, the document [an administrative separation document from Alexis’ Navy commander trying to force Alexis from the Navy] was not signed, dated, or sent. Instead, on January 31, 2011, Alexis received an honorable discharge with a Reentry Code of RE-1, designating that he was eligible to re-enlist without restriction” (H. Rep., 2014, p. 6).
4. Aaron Alexis could have been stopped—either by a thorough investigation of his background prior to granting him a clearance, continuous evaluation of his competency for a security clearance while he was a Naval reservist, or reports of his behavior as a government contractor” (H. Rep., 2014, p. 11).
5. “relying on agencies to voluntarily provide information on investigation quality may not reflect the quality of OPM’s total investigation workload” (*Safeguarding Our Nation’s Secrets: Examining the Security Clearance Process*, 2013, p. 53).
6. “relying on agencies to voluntarily provide information on investigation quality may not reflect the quality of OPM’s total investigation workload” (*The Navy Yard Tragedy*, 2013, p. 87).
7. “the clearance revocation process could potentially be inconsistent with the executive orders in two areas: having an opportunity to be provided with certain information upon which a revocation appeal determination is based, and communicating the right to counsel” (USGAO, 2014b, p. 23).
8. “Communication between personnel security and human capital offices at DHS and DOD varies, but lack of communication between these offices could result in adverse employment actions being taken prematurely or in inappropriate use of personnel security or human capital processes” (USGAO, 2014b, p. 44).
9. “Good human capital policies and practices, to include appropriate practices for evaluating, counseling, and disciplining personnel, are critical factors that affect the quality of internal controls. Moreover, to run and control operations and achieve goals, agencies must have relevant, reliable, and timely communications relating to internal as well as external events; effective communications should occur in a broad sense, with information flowing down, across, and up the organization” (USGAO, 2014b, p. 45).

10. “A lack of communication between the human capital and personnel security offices could result in adverse employment actions being taken prematurely or in the inappropriate use of personnel security processes in lieu of human capital processes” (USGAO, 2014b, p. 46).
11. “To facilitate coordination between personnel security and human capital offices regarding how a security clearance revocation should affect an employee’s employment status, and to help ensure that individuals are treated in a fair and consistent manner, we recommend that • the Secretary of Homeland Security direct the Under Secretary for Management to review and revise policy regarding coordination between the personnel security and human capital offices to clarify what information can and should be communicated between human capital and personnel security officials at specified decision points in the revocation process, and when that information should be communicated; and • the Secretary of Defense direct the Under Secretary of Defense for Personnel and Readiness, in consultation with the Under Secretary of Defense for Intelligence, to review and revise policy regarding coordination between the personnel security and human capital offices to clarify what information can and should be communicated between human capital and personnel security officials at specified decision points in the revocation process, and when that information should be communicated” (USGAO, 2014b, p. 57).
12. “DOD’s comments reflect internal disagreement, which corroborates our finding that there is disagreement within DOD on the legal authority, risks, and benefits of consolidating the department’s multiple appeals boards” (USGAO, 2014b, p. 60).
13. “I would just say that this will only get fixed if we work together, and I mean between branches on this and with the private sector” (*Safeguarding Our Nation’s Secrets: Examining the National Security Workforce*, 2013, p. 27).
14. When trying to act on orders from 10450 to limit national security designations, "It is our understanding that what ensued was essentially a turn battle between OPM and the Director of National Intelligence (DNI), both of which claimed jurisdiction over the boundaries for these positions. OPM's 2012 proposed rule was never finalized" (*Safeguarding Our Nation’s Secrets: Examining the National Security Workforce*, 2013, p. 71).
15. “While agencies performed two of the eight key steps in all cases, most were inconsistent in performing the remaining steps for the oversight of the selected contractor-operated systems. Specifically:• Communicate requirements to contractors…while the contract for one of the systems at DOT was modified to include requirements for background investigations, there was no language included that communicated agency security and privacy requirements. Officials for both agencies were not able to explain why this language was not included in the contracts. Without specific security requirements in the contract, these two systems are at an increased risk that contractors may not understand the requirements that they are expected to implement or cannot be held to the security and privacy requirements during contract performance” (USGAO, 2104a, pp. 14-15).
16. Mr. HUDSON. Thank you. Mr. Marshall, according to several news reports, radios failed law enforcement once they got inside the facility that day…Mr. MARSHALL. Well, let me caveat my answer, Congressman, with, first of all, I haven’t been briefed on the Navy Yard incident first-hand, so everything I know about what happened there, is anecdotal. But I—what I can speak on interoperability to some degree: We learned some lessons, obviously, from 9/11, about the inability of the NYPD and FDNY to interoperate during that incident, so much so that it caused a lot of State and local police departments around the United States to address that issue” (*Facility Protection*, 2013, p. 38).
17. “In my State, the Palmetto State, South Carolina, we learned after Hurricane Hugo that law enforcement needs to be able to communicate all across the State. I believe with a homeland security grant back after 9/11, the State of South Carolina went to an 800-megahertz radio system that we had highway patrol and DNR, and local sheriffs’ agencies were all able to communicate in the event of an emergency” (*Facility Protection*, 2013, p. 44).

APPENDIX K

OVERSIGHT (ABRIDGED)

Oversight - 354

- Audits - 42
    - Definition: Financial audits of OPM's budget can provide oversight of OPM.
    - Rules: Passages discussing financial audits.
        - H.R. 2860 - 12
        - S. 1276 - 10
        - S. 2863 - 2
        - General Concern - 18
- Contractors – 18
    - Definition: Contractors need to be watched.
    - Rules: Passages calling for the review of contractors.
        - Contractors - 18
- Metrics - 28
    - Definition: There needs to be measurement of OPM's investigative process.
    - Rules: Passages discussion metrics.
        - Overall BI (many concerns) – 15
        - Quality in particular - 7
        - Reciprocity in particular - 1
        - Revocation in particular - 5
- Oversight/review - 81
    - Definition: There needs to be more monitoring of OPM.
    - Rules: Passages discussing more oversight and review of OPM.
        - Agencies - 42
        - Continuous evaluation - 3
        - Facilities - 1
        - General concerns - 18
        - OPM - 15
        - Tech oversight - 1
        - Voluntary is problem for oversight - 1
- Quality - 35
    - Definition: There needs to be more data kept about investigation quality.
    - Rules: Passages discussion quality.
        - Agencies - 13
        - Problems - 6
        - OPM - 4
        - Review - 2
        - Quality control - 2
        - Stats - 1
        - Tech - 1
        - Timeliness - 6
- Reports – Need more - 9
    - Definition: More reports are needed to keep track and monitor the BI process.
    - Rules: Passages calling for more reports were included.
        - H.R. 490 - 2
        - S. 1744 - 1
        - S. 2863 – 6
- Standardization – 112
    - Definition: BI processes need to be standardized.
    - Rules: Passages calling for or implying there are standards or standards need improvement.
        - Absence of government standards - 103
        - Followed standards - 3
        - Go beyond standards? - 1

        - Legislation - 4
        - Questions of standards - 1
- Training - 14
    - Definition: Uniform training will help insure investigations correctly carried out.
    - Rules: Passages discussing training.
        - More training is needed for uniformity - 14
- Transparency - 15
    - Definition: BI processes and finances should be open and available for those that need and should access information.
    - Rules: Passages discussing transparency.
        - Costs of OPM products – 11
        - Processes – 4

Audits

H.R. 2860

1. “H.R. 2860 responds to the Office of Personnel Management Inspector General\'s call for increased oversight of the OPM\'s revolving fund by providing the IG access to a portion of that revolving fund moneys for oversight” (114th Cong. Rec, 2014).
2. “Such budget shall include an estimate from the Inspector General of the Office of the amount required to pay the expenses to audit, investigate, and provide other oversight activities with respect to the fund and the activities financed by the fund” (114th Cong. Rec, 2014).
3. "(C) The amount requested by the Inspector General under subparagraph (B) shall not exceed .33 percent of the total budgetary authority requested by the Office” (114th Cong. Rec, 2014).
4. “The revolving fund budget has grown significantly over the past 15 years, from $191 million to more than $2 billion today. OPM\'s revolving fund budget is almost 91 percent of OPM\'s budget; yet the resources available for the IG to audit these funds have not kept pace with the growing amounts” (114th Cong. Rec, 2014).
5. “Last year, OPM Inspector General McFarland informed the Committee on Government Oversight and Reform of what he described as a "serious problem" inhibiting his ability to perform the duties and responsibilities of his office. McFarland stated his office was at a point where it could not meet its statutory obligation to effectively oversee revolving fund activities. He noted that his office had been "inundated with requests from OPM to audit and/or investigate different parts of revolving fund programs," from technical audit work to the continuing flow of allegations involving falsifications of background investigations and abuse of authority” (114th Cong. Rec, 2014).
6. “Inspector General McFarland testified before the Federal Workforce Subcommittee in June, and he said the OPM\'s revolving fund programs "have been operating in the shadows for too long," adding the often-cited phrase "sunshine is the best disinfectant” (114th Cong. Rec, 2014).
7. “H.R. 2860 recognizes oversight as a legitimate business cost by using existing funds to help the IG respond to the increased referrals of alleged fraud within the OPM\'s revolving fund operations, including especially in the background investigation used to determine an individual\'s eligibility for a security clearance” (114th Cong. Rec, 2014).
8. “H.R. 2860 would allow the OPM IG to use a portion of the revolving fund moneys to pay for related audit and investigation work. The OPM IG\'s resources would be limited to one-third of 1 percent of the revolving fund budget, and the IG would be required to submit an annual budget request and report detailing its revolving fund oversight work” (114th Cong. Rec, 2014).
9. “H.R. 2860 provides resources for critical oversight that can be accomplished at relatively low cost, using existing funds” (114th Cong. Rec, 2014).

10. “Through the revolving fund, OPM provides approximately $2 billion in services to agencies on a fee-for-service basis. These services include background investigations, leadership training, and human resource management” (114th Cong. Rec, 2014).
11. “H.R. 2860 would fix the loophole in the current law which prevents this $2 billion revolving fund from paying for the costs of the OPM Inspector General to properly oversee the fund\'s activities” (114th Cong. Rec, 2014).
12. Regarding “OPM IG Act: H.R. 2860, to amend title 5, United States Code, to provide that the Inspector General of the Office of Personnel Management may use amounts in the revolving fund of the Office to fund audits, investigations, and oversight activities, by a \2/3\ yea-and-nay vote of 418 yeas with none voting ``nay''” (OPM IG Act, 2014).

S. 1276

1. The purpose of “bill (S. 1276) [is] to increase oversight of the Revolving Fund of the Office of Personnel Management, strengthen the authority to terminate or debar employees and contractors involved in misconduct affecting the integrity of security clearance background investigations, enhance transparency regarding the criteria utilized by Federal departments and agencies to determine when a security clearance is required, and for other purposes, having considered the same, reports favorably thereon with an amendment in the nature of a substitute and recommends that the bill, as amended, do pass” (S. 113-111, 2014).
2. “to ensure that the Office of Personnel Management\'s (OPM\'s) Inspector General (IG) has the authority to obtain funding needed to audit and investigate critical OPM activities that are currently off limits to oversight by the IG due to an existing lack of authority” (S. 113-111, 2014).
3. “OPM oversees human resources-related matters for federal employees, such as hiring and benefits, as well as the pension and insurance plans for federal retirees. It also provides a range of commercial-like services to other federal agencies including human resource management, leadership training, and background investigations for security clearances. For these services, OPM collects customer-agency\'s funds and deposits them into a Revolving Fund, which in turn pays for the personnel and other resources OPM uses to do its work for other agencies. Because OPM\'s IG may currently not access Revolving Fund money to cover the costs of oversight, the IG is left to operate without the resources or personnel required to carry out thorough oversight of this $2 billion Revolving Fund and the services administered out of the Fund. S. 1276 will remedy this problem by authorizing the use of the Revolving Fund to pay for OPM\'s IG to audit and investigate OPM activities paid for out of that Fund” (S. 113-111, 2014).
4. “Witnesses from OPM and FIS testified that while FIS used OPM\'s Revolving Fund to collect payments from federal agencies to finance background investigations, the Fund has never been audited in its entirety because the costs of audits, investigations, and other oversight activities are prohibited from being charged against the Fund. At the hearing, due to the many concerns raised about the quality of the background investigations being carried out by OPM, the OPM Inspector General, Patrick E. McFarland, testified that the current insufficient level of oversight of the Fund and activities carried out with its resources was a ``clear threat to national security” (S. 113-111, 2014).
5. “OPM devotes more resources to administering the programs funded through the $2 billion Revolving Fund than to any of its other operational programs. Because of the security and fiscal implications of properly administering and financing this Fund, thorough oversight is a critical necessity” (S. 113-111, 2014).
6. “S. 1276 would ensure that such oversight occurs. It does so by authorizing Revolving Fund monies to be spent on the costs of audits, investigations, and oversight activities by the IG. This same legislative proposal was included in the President's Fiscal Year 2014 budget request” (S. 113-111, 2014).

7. “Because OPM\'s IG may currently not access Revolving Fund money to cover the costs of oversight, the IG is left to operate without the resources or personnel required to carry out thorough oversight of this $2 billion Revolving Fund and the services administered out of the Fund. S. 1276 will remedy this problem by authorizing the use of the Revolving Fund to pay for OPM\'s IG to audit and investigate OPM activities paid for out of that Fund” (S. 13-111, 2013).
8. “S. 1276 would ensure that such oversight occurs. It does so by authorizing Revolving Fund monies to be spent on the costs of audits, investigations, and oversight activities by the IG” (S. 13-111, 2013).
9. In the bill, section 2 “section 5 U.S.C. Sec. 1304(e), to authorize the costs of OPM Inspector General audits, investigations, and oversight activities relating to the Revolving Fund and the functions financed by the Fund, to be charged against the Fund” (S. 13-111, 2013).
10. This bill says to make the “Fund available to OPM for the cost of audits, investigations, and oversight that are conducted by OPM\'s IG and that relate to the Fund and the functions financed by the Fund…[and] specifies that the estimate from OPM\'s IG may not exceed 0.33 percent of the total amount of expected expenditures from the Revolving Fund that OPM includes in the budget for Congress” (S. 13-111, 2013).

APPENDIX L

REQUIREMENTS DETERMINIATION (ABRIDGED)

- Amount of classified info - 21
    - Definition: The amount of classified information is vast and too large.
    - Rules: Passages discussing the amount of classified information and/or that there is too much classified.
        - S. 2683 - 2
        - General Overview - 5
        - Motives - 7
        - Number a concern - 5
        - Snowden - 2
- Position designation/# of clearances - 109
    - Definition: There amount of positions designated as needing a clearance is vast, and there are too many clearances needed.
    - Rules: Passages discussing the amount of classified jobs and/or that there are too many people with these positions.
        - 9/11 - 11
        - S. 1744 - 4
        - S. 2683 - 2
        - Need standards - 40
        - Vulnerable/why vulnerable - 25
        - Why so many - 27
- Facilities - 29
    - Definition: Facilities are evaluated to determine if they need clearances.
    - Rules: Passages discussing facilities were included.
        - Access - 29
- National security state - 10
    - Definition: Too much information is classified leading us to become a national security state.
    - Rules: Passages using the words “national security state” were included.
        - Too much classification - 10

Amount of classified info

S. 2683

1. S. 2683 – the CORRECT Act recommends: 3. “Ten percent reduction in holdings of classified information - the president should reduce "classified information, through declassification and improved original and derivative classification decision making, by not less than ten percent as compared to the amount of such information as of the day before such date" (S. 2683, 2014).
2. S. 2683 – the CORRECT Act recommends: “a position shall only be designated as a national security position if access to classified information is required or if that position--(1) presents a risk of a material adverse effect on the national security (as described in section 732.201 of title 5, Code of Federal Regulations, or similar successor regulation); and (2) is determined to be a public trust position" (S. 2683, 2014).

General overview

1. “Given the increasing amount of classified information produced and maintained by our government and the increasing number of folks with access to that information, we have a real problem on our hands if we cannot get this right. And because of the national security implications involved, there is simply no margin for error” (*Safeguarding Our Nation’s Secrets: Examining the Security Clearance Process*, 2013, p. 2).
2. “Two problems. One, there is way too much stuff that is classified that does not need to be classified. And, two, there are way too many security clearances approved. So if you markedly increase the amount of material that does not need to be classified, you have to

increase the number of people that need to have access to it." (*The Navy Yard Tragedy*, 2013, p. 4).

3. "We classify way too much stuff… Because once you create something that is classified, the only people that can work on it are people that have a clearance for that classification or above" (*The Navy Yard Tragedy*, 2013, p. 22).
4. There is a government-wide classification system for information, but agencies can also decide what information should be classified (*The Navy Yard Tragedy*, 2013, p. 128).
5. "But on over classification or on classification…It is a concern, one, because it is hard for people we represent, our constituents, to have access to this information to understand how the government works and how it is conducting itself" (*Safeguarding Our Nation's Secrets: Examining the National Security Workforce*, 2013, p. 17).

APPENDIX M

APPLICATION (ABRIDGED)

- **Forms**
  - Definition: The investigative paperwork needs reform.
  - Rules: Passages dealing with the form.
    - Reform the forms. - 3
- **Reciprocity**
  - Definition: Agencies need to share data about acceptance/ honoring of another agency's investigation and granting of a clearance -it may also be a risk not to.
  - Rules: Passages dealing with reciprocity.
    - Matters of reciprocity. - 15

Forms

Reform the forms

1. "He had already filed his electronic version of an SF86. But it was somewhere on a government computer and could not be retrieved. He had to fill it out again, a 4-hour process. His subsequent review was a government employee or a contract employee going through question by question. He contrasts that with his experience in the private sector, answering five questions which had a 99-percent reveal rate in terms of whether that person was committing fraud" (*Safeguarding Our Nation's Secrets: Examining the Security Clearance Process*, 2013, p. 5).
2. There needs to be reform of the SF-86. "It is imperative that we collect accurate information pertinent to today's security and counterintelligence concerns" (*The Navy Yard Tragedy*, 2013, p. 67).
3. The idea of "Four Ones" is "one application, one investigation, one adjudication and one clearance" (*The Navy Yard Tragedy*, 2013, p. 99).

Reciprocity

Matters of reciprocity

1. Regarding re-investigations and movement between companies and positions, "Certainly what the chairman brought up in entities not reporting, again, garbage in, garbage out, we won't know, but I think for improvement we need to look at if they shift positions, the contractor should do a review" (*DC Navy Yard Shooting*, 2014, p. 51).
2. "Although executive branch agency officials have stated that reciprocity is regularly granted as it is an opportunity to save time as well as reduce costs and investigative workloads, we reported in 2010 that agencies do not consistently and comprehensively track the extent to which reciprocity is granted government-wide" (*DC Navy Yard Shooting*, 2014, p. 170).
3. Problems "include incomplete and poorly synchronized fielding of electronic case management systems and other tools across government, shortcomings in metrics for reciprocity, a sound requirements process to determine positions that require a clearance, and most troubling, I think, is the pressure to meet timeliness metrics impacting the quality of investigations" (*Safeguarding Our Nation's Secrets: Examining the Security Clearance Process*, 2013, p. 4).
4. "Senator TESTER. Very quickly, Mr. Miller, should I be concerned about this, concerned that there is no apparent metrics or standards or——Mr. MILLER. Sir, there are standards. Senator TESTER. Yes, but they vary between each agency, so consequently there is no reciprocity, and the standards could go from soup to nuts" (*Safeguarding Our Nation's Secrets: Examining the Security Clearance Process*, 2013, p. 23).
5. "One of the areas we have concerns is on metrics….and this covered not only timeliness but the investigations, the adjudications, and reciprocity…But those metrics, as I have noted, with the exception of timeliness, have not been fully developed" (*The Navy Yard Tragedy*, 2013, p. 18).

6. “executive branch agencies have not fully developed and implemented metrics to measure quality in key aspects of the personnel security clearance process, including: (1) investigative reports; (2) adjudicative files; and (3) the reciprocity of personnel security clearances” (*The Navy Yard Tragedy*, 2013, p. 85).
7. “we reported in 2010 that agencies do not consistently and comprehensively track the extent to which reciprocity is granted government-wide (*The Navy Yard Tragedy*, 2013, pp. 89-90).
8. “Without comprehensive, standardized metrics to track reciprocity and consistent documentation of the findings, decision makers will not have a complete picture of the extent to which reciprocity is granted or the challenges that agencies face when attempting to honor previously granted security clearances” (*The Navy Yard Tragedy*, 2013, pp. 90-1).
9. "...even after significant intra-governmental effort, meaningful reciprocity remains elusive" (*The Navy Yard Tragedy*, 2013, p. 99).
10. Barriers to reciprocity are the doubt of quality/comprehensiveness of another agency's investigation and application of suitability concerns specific to the receiving agency (*The Navy Yard Tragedy*, 2013, p. 125).
11. “They said that they would like to establish and make more robust metrics for reciprocity, quality, and out-of-scope periodic reinvestigations, and from there it would be a natural progression to look at developing some metrics for revocations and denials, and other areas. However, they stated that due to constrained resources and other priorities they were uncertain whether they could make a business case to allocate the resources” (USGAO, 2014b, p. 39).
12. “In an environment where reciprocity of personnel security clearances is required among federal agencies, the consistent and transparent application of the processes governing whether individuals should retain their access to classified information has become increasingly important, so that all agencies can have reasonable assurance that only trustworthy individuals obtain and keep security clearances” (USGAO, 2014b, p. 53).
13. “The proposed regulation is not intended to increase or decrease the total number of national security-sensitive positions within the Federal Government; but, rather, to ensure that each position is designated accurately. The intent is to issue national-level policy guidance to promote consistency in designating positions and address changed national security concerns post-9/11. This approach will improve consistency and the level of investigation performed for similar positions in other agencies; thereby, promoting efficiency and facilitating reciprocity” (*Safeguarding Our Nation’s Secrets: Examining the National Security Workforce*, 2013, p. 4).
14. “On the Defense Authorization Bill, which is on the floor this week, we have an amendment that asks GAO to examine quality metrics and reciprocity as it pertains to the process. And along those same lines, we asked OMB’s Performance Accountability Council (PAC) to examine how we can improve the processes for access to State and local law enforcement records in the background investigation process” (*Safeguarding Our Nation’s Secrets: Examining the National Security Workforce*, 2013, p. 16).
15. “But what I know through the media accounts and some anecdotal comments or conversations I have had with other people, from what I know, Mr. Alexis had a security clearance with the Navy. When he left the Navy, it was still an in-scope clearance, meaning that the investigation was within the required time frame in order for the organization he was going to to accept that investigation on reciprocity. We are required by Executive Order in the Federal Government to accept security clearances on reciprocity if there is an investigation that we can point to. The one thing about reciprocity is that we are also required to accept it on its face. We are not allowed to do any additional checks unless we have information—derogatory information to the contrary. So, it looks to me, not having been briefed, that the contracting company accepted Mr. Alexis’s security clearance on reciprocity, which was one gap, without having to do additional checks. That also there was a faulty investigation. There

was information within the investigation that was done by a private contractor that wasn't accurate. So, it was almost like a perfect storm. It was a gap that was— it was unfortunately hard to overcome. Mr. DUNCAN. Yes, we are human. I get that" (*Facility Protection*, 2013, p. 46).

APPENDIX N

INVESTIGATION (ABRIDGED)

- Contractors - 41
  - Definition: Contractors cause problems with BIs.
  - Rules: Passages discussing contractors in the context of a flawed BI.
    - Contractors causing trouble for government - 7
    - Different standards? - 7
    - Government IT systems - 14
    - Government problem with contractors – 12
    - Less quality - 1
- Fraud - 38
  - Definition: Fraud causes issues for BIs.
  - Rules: Passages discussing fraud in BIs.
    - Contractor - 11
    - Employee - 7
    - Federal legislation - 6
    - General - 14
- Incomplete investigations - 25
  - Definition: Some investigations are turned in with incomplete information.
  - Rules: Passages discussing incomplete investigations and what is often incomplete.
    - Amount - 11
    - Using incomplete information - 14
- Internet/social media - 7
  - Definition: Use of the internet and social media is not incorporated in the BI.
  - Rules: Passages discussing the use of Internet information.
    - No use of Internet - 7
- Law enforcement - 52
  - Definition: Law enforcement data is often hard to get and may be incomplete.
  - Rules: Passages discussing law enforcement issues.
    - Can't get information - 24
    - Consequences – 6
    - Don't have to get - 5
    - Fail to get/report information - 17
- Mental health - 19
  - Definition: Mental health data is often hard to get and may be incomplete.
  - Rules: Passages discussing issues with mental health information.
    - Complex issue - 8
    - General - 7
    - In hindsight - 4
- Tax debts/debts - 29
  - Definition: Tax and debt data is often hard to get and may be incomplete.
  - Rules: Passages discussing problems getting tax information.
    - Hard to get tax information - 29
- USIS - 48
  - Definition: Specifically, the contractor USIS is a weakness for the BI.
  - Rules: Passages discussing USIS and its associated BI issues.
    - Conflict of interest - 9
    - Falsification - 30
    - Faulty work - 9

Contractors

Contractors causing trouble for government

1. "The Inspector General of OPM, Patrick McFarland, testified at the hearing about the fabrication of background investigations within OPM\'s Federal Investigative Services. Mr.

McFarland stated that ``one of the most flagrant criminal violations that we encounter is the falsification of background investigation reports\'\' and that there are situations where the ``Federal Investigative Services\' background investigators, either Federal employees or contractors, report interviews that never occurred, record answers to questions that were never asked, and document records checks that were never conducted" (S. 113-276, 2014).

2. "Further troubling allegations questioning the integrity of the background check program emerged on October 30, 2013, when the Department of Justice joined a civil fraud lawsuit claiming that a contractor, which was performing a large share of the investigative work contracted out by OPM and other agencies, had engaged in a systemic failure to adequately conduct security clearance background investigations." Senior management at the contractor dumped at least 665,000 incomplete cases (about 40%) from 2008 to 2012 (S. 113-276, 2014).
3. "On the other hand, what we are doing now is the worst of all situations because we are giving the impression that all these millions of people who have security clearances, we have checked them out. We are confident that they are mentally stable, they are not criminals, and they obey the law. We have no idea if that is true. We are clueless as to whether or not that is true, because this process has become in a way a pro forma kind of process with contractors. And the reason the contractors were off the reservation is because they bid an amount and that contractor wanted to make money, so that was time to cut corners. You wanted to make your number? You wanted to make money? Well, then, you did not have to do the whole thing. You just turned it in and pretended like you did" (*The Navy Yard Tragedy*, 2013, p. 33).
4. On average weekly, OPM gets about 55,000-60,000 field work cases completed by contractors, and approx. 3.3% is returned for not meeting standards (*The Navy Yard Tragedy*, 2013, p. 118).
5. "One of the things—when they were talking with you about background investigations and security clearances, you said you would hold the contractor responsible. I have heard that a lot in the last 10 years up here. What does that mean to you—holding a contractor responsible? Does that mean terminating the contract? Does that mean taking the contractor to court to get damages for when they did not perform? What does that mean to you? Ms. ARCHULETA. Senator, it means to me that in the review of the information or evidence, if a contractor has not performed or has falsified information; there would be a review of that contract and his or her performance, and appropriate actions would be taken. In some cases, that would mean debarment" (Nomination of Hon. Katherine Archuleta, 2013, pp. 9-10).
6. "Federal agencies have reported increasing numbers of cybersecurity incidents that have placed sensitive information at risk, with potentially serious impacts on federal operations, assets, and people. Recent national security events involving the unauthorized disclosure of classified federal information have involved contractors and contractor employees" (USGAO, 2014b, p. 7).
7. "Additionally in 2013, it was reported that a National Security Agency contractor employee had released a large of amount of classified National Security Agency surveillance program data" (USGAO, 2014b, p. 8).

Different standards?

1. "The training curriculum is the same for both [contractor and employee]" (*The Insider Threat*, 2013, p. 10).
2. "Can any of you comment on whether there is a different level of quality--better or worse--between the Government carrying out the investigation or private contractors?... First off, there is no difference in the way we clear contract workforce versus Federal workforce relative to background investigations. Second is the quality of investigations are the same. They have got to investigate to the same standards and they have got to meet the same quality standards, both Federal and contract employees" (*The Insider Threat*, 2013, p. 45).

3. Miller responds, “They all have to be trained to the same level, and obviously through the contract process, when they come in to actually compete for the work they all have to meet the same standards when they are selected to do contract work for the Government” (*The Insider Threat*, 2013, p. 45).
4. "training standards for investigators and adjudicators, which also help to ensure that investigations are conducted to consistent standards across all investigating agencies…modeled after our own Federal Investigator Training Program" (*DC Navy Yard Shooting*, 2014, pp. 9-10).
5. Both OPM and contract investigators are trained to the same standards promulgated by OPM, and perform the same work” (H. Rep., 2014, p. 15).
6. Training is the same for both the contractor and employee (*Safeguarding Our Nation’s Secrets: Examining the Security Clearance Process*, 2013, p. 87).
7. For contractors in physical security, “What they are not trained to do is go from room to room trying to find the individual… Now, if they come into contact with a shooter, they will engage. What they will not do today is pursue the active shooter” (*The Navy Yard Tragedy*, 2013, p. 160).

APPENDIX O

ADJUDICATION (ABRIDGED)

- **Adjudication problems**
  - Definition: The process of determining who gets a clearance based on adjudication criteria.
  - Coding Rules: Passages dealing with the problems of adjudication.
    - Lack of information - 29
    - Must be government deciding - 1
    - Results of bad BIs - 4
    - Risks - 7
    - Standards - 20

Adjudication problems

Lack of information

1. Regarding neighborhood checks for TS clearances, "particularly in this area people move and there may not be anybody who knew the subject of the investigation who is available, so we have given guidance to the DOD consolidated adjudication facility, which identifies the types of information which may not be available and which would still allow the DOD CAF to do their adjudication" (*DC Navy Yard Shooting*, 2014, p. 66).
2. A 2009 report "identified issues regarding the quality of DOD adjudications. With respect to DOD adjudicative files, in 2009, we estimated that 22 percent of the adjudicative files for about 3,500 initial top secret clearances that were adjudicated favorably did not contain all the required documentation even though DOD regulation requires that adjudicators maintain a record of each favorable and unfavorable adjudication decision and document the rationale for granting clearance eligibility to applicants with security concerns revealed during the investigation." (*DC Navy Yard Shooting*, 2014, p. 166).
3. Adjudicators would often like the actual records, and "according to Defense Office of Hearings and Appeals officials, in one case, an investigator's summary of a police report incorrectly identified the subject as a thief when the subject was actually the victim." (*DC Navy Yard Shooting*, 2014, p. 167).
4. "However, we also found that the shared information available to adjudicators contains summary-level detail that may not be complete. As a result, agencies may take steps to obtain additional information, which creates challenges to immediately granting reciprocity." (*DC Navy Yard Shooting*, 2014, p. 172).
5. "Enhancing federal agencies' access to tax-debt information for the purpose of both investigating and adjudicating security-clearance applicants, as well as ongoing monitoring of current clearance holders' tax-debt status, would better position agencies to make fully informed decisions about eligibility" (USGAO, 2013, p. 27).
6. "Key information sometimes does not reach the agency adjudicators, which means that individuals—such as Aaron Alexis—are occasionally granted clearances that, had the adjudicator been aware of all the pertinent information, should have received more scrutiny and could have been denied" (H. Rep, 2014, p. 2).
7. Despite Alexis' behavior, "None of this information was ever given to an adjudicator who had the ability to pull Alexis' Secret level clearance, which he maintained until September 16, 2013" (H. Rep, 2014, p. 2).
8. "Legislation could also finally allow agency adjudicators to directly speak with OPM investigators, giving adjudicators additional information on an applicant when deciding whether or not to grant a clearance" (H. Rep, 2014, p. 3).
9. "this information on Alexis' mental state did not get to Department adjudicators, who could have taken steps to suspend or terminate his security clearance" (H. Rep, 2014, p. 11).
10. "DOD adjudicators who granted Alexis' clearance. They explained that 70 to 80 percent of all investigative files sent by OPM are missing at least some information. The file is frequently

missing financial information, such as documentation of debt repayment or payment arrangements" (H. Rep, 2014, p. 30).

11. Requesting more information slows down the case. "Requesting additional information from OPM requires that OPM reopen the case, contact and potentially interview the subject, close the case, and send the information back to the adjudicator" (H. Rep, 2014, p. 30).
12. "would be extremely helpful if investigative reports to included actual records, including arrest records and financial records showing timely debt repayment, as opposed to simply an investigator summary of the records" (H. Rep, 2014, p. 30).
13. Regarding the use of the Internet, "Unfortunately, investigators conducting federal security clearance background checks do not see, search, or receive reports of the vast amount of information available online. Nor do current federal security process guidelines allow the adjudicators who grant the clearances to access this information" (H. Rep, 2014, p. 36).
14. "Currently, agency adjudicators do not speak with the OPM or contract investigators who investigated a security clearance application… Adjudicators cannot simply contact investigators to ask follow-up questions about the file. The ability to do so would be extremely helpful to adjudicators in certain instances." (H. Rep, 2014, p. 38).
15. "And I am wondering about whether you are measuring those metrics [on quality]. You have been pressed on timeliness, I am sure, but here is some data. In 2009, GAO assessed from a sample that 87 percent of investigative reports that DOD adjudicators used to make clearance decisions were missing background documentation—87 percent. GAO subsequently recommended OPM measure the frequency with which investigative reports meet Federal investigative standards" (*Safeguarding Our Nation's Secrets: Examining the Security Clearance Process*, 2013, p. 16).
16. "Ms. FARRELL. The documentation was not in the files. We recognize that it may be challenging to track down people who may be deployed, and if the documentation is there, then that could explain it. We found the same types of incomplete documentation with DOD's adjudication files. We recommended they offer guidance in these situations, and that if there are difficulties, you document it so that the adjudicator or whoever does a review will know why that was left blank, the person was deployed" (*Safeguarding Our Nation's Secrets: Examining the Security Clearance Process*, 2013, p. 17).
17. When information isn't able to obtained due to the voluntary nature of BIs, "the best that OPM can do is to make its best effort to locate relevant information through alternative means, and provide notations concerning what is missing" (*Safeguarding Our Nation's Secrets: Examining the Security Clearance Process*, 2013, p. 83).
18. Regarding GAO's study about missing case information, the type of information missing is "Employment verification and discussions with the employers; social references, especially the number of social references in order to determine someone's character; completeness of the application, which should be the very first step, as we have noted before, that should be done before OPM even moves forward" (*The Navy Yard Tragedy*, 2013, p. 40).
19. "GAO's 2009 report also identified issues with the quality of DOD adjudications. Specifically, GAO estimated that 22 percent of about 3,500 initial top secret clearances that were adjudicated favorably did not contain all the required documentation" (*The Navy Yard Tragedy*, 2013, p. 73).
20. "executive branch agencies have not fully developed and implemented metrics to measure quality in key aspects of the personnel security clearance process, including: (1) investigative reports; (2) adjudicative files; and (3) the reciprocity of personnel security clearances" (*The Navy Yard Tragedy*, 2013, p. 85).
21. "deficiencies in investigative reports affect the quality of the adjudicative process…For example, some agency officials noted that OPM investigative reports do not include complete copies of associated police reports and criminal record checks" (*The Navy Yard Tragedy*, 2013, p. 87).

22. Adjudicators need copies of reports because “For example, according to Defense Office of Hearings and Appeals officials, in one case, an investigator’s summary of a police report incorrectly identified the subject as a thief when the subject was actually the victim.” (*The Navy Yard Tragedy*, 2013, p. 88).
23. “we recommended that DOD issue guidance to clarify when adjudicators may use incomplete investigative reports as the basis for granting clearances” (*The Navy Yard Tragedy*, 2013, p. 89).
24. "Improving information sharing of information relevant to adjudications as it becomes available while reducing duplication in our current processes is a top priority of this Review, as is avoiding duplication as we explore IT capabilities (*The Navy Yard Tragedy*, 2013, p. 115).
25. On average weekly, OPM gets about 55,000-60,000 field work cases completed by contractors, and approx. 3.3% is returned for not meeting standards (*The Navy Yard Tragedy*, 2013, p. 118).
26. In response to GAO's assessment of incomplete investigations, OPM specified that “gathering all the information required by the federal investigative standards does not necessarily indicate a quality investigation"...and that "an investigative report that includes all of the items required by the federal investigative standards does not equate to having obtained the right or best sources of information about an applicant” Overall, OPM disagreed with the extent that GAO assessed OPM's cases deficient (*The Navy Yard Tragedy*, 2013, p. 136).
27. When judging completeness, OPM goes by investigative standards as well as a case-by-case consideration. I.e., even though an applicant is required, there are instances where the applicant is deployed and unreachable. The GAO considers these evaluations as not data-driven (*The Navy Yard Tragedy*, 2013, p. 136).
28. In 2010, the GAO reported challenges facing agencies implementing timeliness objectives from the IRTPA 2004 was investigation quality and cost, and DHS, DOE, Treasury, DOJ and four areas of the DOD reported deficient investigative reports which leads to slower adjudications. This incompleteness may also result in clearances being given to untrustworthy individuals (*The Navy Yard Tragedy*, 2013, p. 137).
29. The DOD sometimes does their own BI work to fill in the gaps for OPM’s deficient reports to be more timely in adjudications (*The Navy Yard Tragedy*, 2013, p. 138).

Must be government deciding

1. S. 2683 – the CORRECT Act recommends: 7. “Automated or nongovernmental adjudication prohibited –“An adjudication by an agency that an individual may not have access to classified information may only be made by a Federal employee and may not be rendered by an automated, electronic, or computer system” (S. 2683, 2014).

APPENDIX P

APPEALS (ABRIDGED)

- Revocation/suspension/ appeals - 54
    - Definition: The penalties for adverse actions are not uniform.
    - Rules: Passages discussing corrective matters for clearances.
        - Contractor and employees - 8
        - Inconsistent implementation-12
        - OPM – Lack of program- 4
        - Oversight-14
        - Punishment-5
        - Uniform criteria-11
- Safeguard for employees - 67
    - Definition: Employees need protections from some measures.
    - Rules: Passages that talk about employee rights.
        - S. 2683 - 4
        - Appeal serious actions - 1
        - Due process - 1
        - Employees - 7
        - Inappropriate actions taken - 3
        - Kaplan v. Conyers - 21
        - Less safe - 2
        - Merit Systems Protection Board - 15
        - Right to counsel - 2
        - Uniform standards - 11

Revocation/ suspension/ appeals

Contractor and employees

1. “Contractors employing cleared individuals do not receive copies of warning letters. The letter is instead sent to the security officer of the agency holding the contract.” so the actual employer doesn’t know if the clearance was conditional (H. Rep. 2014, p. 31).
2. “One of the things—when they were talking with you about background investigations and security clearances, you said you would hold the contractor responsible. I have heard that a lot in the last 10 years up here. What does that mean to you—holding a contractor responsible? Does that mean terminating the contract? Does that mean taking the contractor to court to get damages for when they did not perform? What does that mean to you? Ms. ARCHULETA. Senator, it means to me that in the review of the information or evidence, if a contractor has not performed or has falsified information; there would be a review of that contract and his or her performance, and appropriate actions would be taken. In some cases, that would mean debarment” (Nomination of Hon. Katherine Archuleta, 2013, pp. 9-10).
3. When Federal employees are suspected of falsification, they are placed on administrative leave until the case is resolved and evidence is gathered to support being fired, while still getting paid. Contractors are immediately removed from contracts. Archuleta believes agencies need to hold employees engaging in misconduct accountable, but it is also important to give these employees due process (Nomination of Hon. Katherine Archuleta, 2013, p. 81).
4. “Ordinarily, most federal civilian employees have a right to appeal serious adverse employment actions taken against them to the Merit Systems Protections Board. However, in the security clearance context, federal case law [see Navy v. Egan, 484 U.S. 518 (1988), and Kaplan v. Conyers, 733] has limited the scope of the board’s review of adverse actions. Specifically, the board may review appeals of adverse employment actions resulting from a denial or revocation of a security clearance or a determination that an employee is not eligible

to hold a sensitive position for specific procedural issues, but the board cannot review the substance of a security clearance denial or revocation, or a finding that an employee is not eligible to hold a sensitive position." (USGAO, 2014b, p. 47).

5. "The Conyers' ruling rejected the text, the structure, and the history of the Civil Service Reform Act (CSRA), along with the plain language of Egan to hold that the MSPB may not review the merits of an agency determination that an employee is ineligible to hold a sensitive position" (*Safeguarding Our Nation's Secrets: Examining the National Security Workforce*, 2013, pp. 10-11).
6. "By eliminating the Board from the equation, employees will have no forum in which to obtain independent, meaningful review of agency actions arising from the denial or loss of eligibility to occupy a sensitive position or the denial or loss of a security clearance" (*Safeguarding Our Nation's Secrets: Examining the National Security Workforce*, 2013, p. 282).
7. "But if they [agencies] can arbitrarily do what they want as far as determining which positions are sensitive, because they can find something out there that would do that—I mean, the example of food was a fine example because we all eat—why—I guess the question is, are we going to end up with another Snowden incident or another Naval Yard shooter incident, because we have so many of these things to do that folks end up cutting corners in the process?...we have a situation where we have so many people out here with security clearances that corners are being cut now to get those clearances done. And a person could deny that, but the proof is in the pudding and look what happened with Alexis" (USGAO, 2014a, p. 23).
8. "will need to propose and issue changes to the Federal Acquisition Regulations that would ``impose those applicable reporting requirements on contractors and to ensure that enforcement and accountability mechanisms are in place" (S. 113-283, 2014).

Inconsistent implementation

1. "Inconsistent implementation of the requirements in the governing executive orders by DHS, DOD, and some of their components, and limited oversight over the revocation process, have resulted in some employees experiencing different protections and processes than other employees" (USGAO, 2014b, p. intro).
2. "Specifically, DHS and DOD have implemented the requirements for the revocation process contained in Executive Orders 12968 and 10865 in different ways for different groups of personnel. Although certain differences are permitted or required by the executive orders, GAO found that implementation by some components could potentially be inconsistent with the executive orders in two areas. As a result, some employees may not be provided with certain information upon which a revocation appeal determination is based, and may not be told that they have a right to counsel" (USGAO, 2014b, p. intro).
3. "These inconsistencies in implementation may be in part because neither DHS nor DOD have evaluated the quality of their processes or developed performance measures to measure quality department-wide. Similarly, the Office of the Director of National Intelligence (ODNI) has only exercised limited oversight by reviewing policies and procedures within some agencies. ODNI has not established any metrics to measure the quality of the process government-wide and has not reviewed revocation processes across the federal government to determine the extent to which policies and procedures should be uniform" (USGAO, 2014b, p. intro).
4. "DHS and DOD employees whose clearances were revoked may not have consistent employment outcomes, such as reassignment or termination, because these outcomes are determined by several factors, such as the agency's mission and needs and the manager's discretion. Further, most components could not readily ascertain employment outcomes of individuals with revoked clearances, because these data are not readily available, and communication between personnel security and human capital offices at the departments varies" (USGAO, 2014b, p. intro).

5. “Implementation of continuous evaluation could prompt further investigation of events and incidents that could lead to an increase in the number of revocations that are proposed by government agencies. In these reports, both OMB and DOD made recommendations related to improving access to information and reducing the number of clearance holders, among other recommendations” (USGAO, 2014b, p. 2).
6. “the clearance revocation process could potentially be inconsistent with the executive orders in two areas: having an opportunity to be provided with certain information upon which a revocation appeal determination is based, and communicating the right to counsel” (USGAO, 2014b, p. 23).
7. “Communication between personnel security and human capital offices at DHS and DOD varies, but lack of communication between these offices could result in adverse employment actions being taken prematurely or in inappropriate use of personnel security or human capital processes” (USGAO, 2014b, p. 44).
8. “the security clearance revocation process implementation differences we identified at DHS and DOD continue in part because ODNI has not reviewed security clearance revocation processes across the federal government to determine the extent to which policies and procedures should be uniform” (USGAO, 2014b, p. 40).
9. “Specifically, ODNI has not assessed whether the existing security clearance framework, with its parallel processes for contractors and government employees, or a single process applicable to all types of employees would best facilitate the effective, efficient, consistent, and timely completion of security clearance revocation proceedings. When asked about the different processes, ODNI officials stated that the executive orders provide broad guidelines that give agencies the flexibility to implement a review and appeal process that best fits the agency’s needs, and there is no single solution that all agencies must follow” (USGAO, 2014b, p. 40).
10. “DHS and DOD employees whose eligibility to access classified information has been revoked may not have consistent employment outcomes, such as reassignment or termination, because these outcomes are generally dependent on several factors, including the agency’s mission and needs and the manager’s discretion” (USGAO, 2014b, p. 41).
11. “A lack of communication between the human capital and personnel security offices could result in adverse employment actions being taken prematurely or in the inappropriate use of personnel security processes in lieu of human capital processes” (USGAO, 2014b, p. 46).
12. “But if they [agencies] can arbitrarily do what they want as far as determining which positions are sensitive, because they can find something out there that would do that—I mean, the example of food was a fine example because we all eat—why—I guess the question is, are we going to end up with another Snowden incident or another Naval Yard shooter incident, because we have so many of these things to do that folks end up cutting corners in the process?...we have a situation where we have so many people out here with security clearances that corners are being cut now to get those clearances done. And a person could deny that, but the proof is in the pudding and look what happened with Alexis” (USGAO, 2014a, p. 23).

APPENDIX Q

PERIODIC REINVESTIGATION (ABRIDGED)

Periodic Reinvestigation -183

- **More/continuous evaluation - 138**
    - Definition: There should be a process that evaluates those with clearances continually, and information should not just be gathered during an investigation.
    - Rules: Passages that discuss continuous evaluation. (Same as surveillance)
        - Definition - 4
        - Drawbacks/Limitations -18
        - Frequency - 11
        - History -8
        - How it works -26
        - Programs -12
        - Real time -14
        - Role of tech -14
        - Why used/justification - generic examples -21
        - Why used – specific examples - 10
- **Time between investigations- 45**
    - Definition: The current time between investigations is inadequate.
    - Rules: Passages discussing the length of investigations and the need to have more frequent investigations.
        - Current - 8
        - What is wanted - 8
        - Who set the 10 year time - 1
        - Why - 28

More/continuous evaluation

Definition

1. “The term \'continuous evaluation\', as defined in Executive Order 13467 (50 U.S.C. 3161 note), means reviewing the background of an individual who has been determined to be eligible for access to classified information at any time during the period of eligibility” (S. 2683, 2014; H.R. 5240, 2014).
2. “Continuous evaluation means reviewing the background of an individual who has been determined to be eligible for access to classified information (including additional or new checks of commercial databases, government databases, and other information lawfully available to security officials) at any time during the period of eligibility to determine whether that individual continues to meet the requirements for eligibility for access to classified information” (USGAO, 2013, p. 9).
3. Per EO 13467 and revised Federal Investigative Standards signed in 2012, "CE allows for a review at any time of an individual with eligibility or access to classified information, or in a sensitive position, to ensure that the individual continues to meet the requirements for eligibility” (*The Navy Yard Tragedy*, 2013, p. 64).
4. “The government has been working to establish automated systems, referred to generally as Continuous Evaluation (CE), to check government and commercial data sources on a more frequent or even continuous basis to flag issues of concern during the period between background investigations” (S. 113-283, 2014).

Drawbacks/Limitations

1. These protections should include “standards for the protection of national security and promotion of fairness, transparency, and employee protections, including safeguards to preserve the rights and confidentiality of whistleblowers with respect to the operation of a continuous evaluation program and the operation of an insider threat program by a Federal agency” (S. 2683, 2014; H.R. 5240, 2014).

2. To curb abuse of CE, agencies must submit “Demographic information on each individual whose eligibility for access to classified information was changed as a result of information collected through the continuous evaluation program or insider threat program, including age, race, gender, and ethnicity. [And] a description of the mechanisms used to conduct the evaluations, including how individuals were selected, whether the evaluations were randomized, and if so, the nature of the randomization, including the degree to which it was temporally randomized and the degree to which the selection of individuals subject to the program was randomized” (S. 2683, 2014; H.R. 5240, 2014).
3. “(B) any covered individual who is not a cleared individual is not subject to continuous evaluation or monitoring” (H.R. 4022, 2014; H.R. 490, 2015).
4. “In 2005, interestingly, a year before Ricky Elder enlisted in the Army, 2 years before Aaron Alexis enlisted in the Navy, and 7 years to the day before Ricky Elder’s deadly attack, the Department of Defense testified to this Committee—and this was in June 2005—about the Automated Continuous Evaluation System, (ACES). And you all said that you were going to continuously evaluate the background and suitability of security clearances. Mr. Prioletti, in your opening—in your written statement—I did not hear you say it in your statement, but in your written statement you noted that 3 years earlier, in 2008—3 years later from the 2005 testimony you gave before this Committee, in 2008 President Bush directed by his Executive Order that an individual who has been determined to be eligible for or currently has access to classified information shall be subject to Continuous Evaluation. That was an Executive Order back in 2008” (*The Navy Yard Tragedy*, 2013, pp. 35-6).
5. Regarding CE, “I know we have heard today, ‘‘We are working on this.’’ I heard in response to an earlier question, ‘‘We have an interagency working group. We are developing a concept of operations.’’ I wrote this down. ‘‘We are doing research.’’ Again, this has been going on now for a decade. If you testified in 2005 it was going on in 2004, it may be more than a decade. So here we are. It is 5 years after the Executive Order, 8 years after this Committee heard about the plans, and we are dealing with the tragedy at the Navy Yard” (*The Navy Yard Tragedy*, 2013, p. 36).
6. “Senator PORTMAN. You were not here in this job 9 years ago when we heard that it was going to be in place by 2005. But you are here now, and so, one question I could ask you is: Why has it taken so long? And you might say, ‘‘I do not know. I was not in charge.’’ But you are in charge now, and you are saying that you are going to have this fully operational in 3 years. Is that correct?” (*The Navy Yard Tragedy*, 2013, p. 37).
7. “Mr. LEWIS. For the Automated Continuous Evaluation System as it currently stands, it is an operational system. It is still in a research and development mode, but it is an operational system. The limits right now—— Senator PORTMAN. I mean, when I say ‘‘operational,’’ I mean it actually would cover more than a small percentage of the people who are in between their clearances. You are talking about taking it from 3,600 up to 100,000. How many security clearances do you have at DOD? Mr. LEWIS. We have about 2.5 million people who are eligible and in access for classified information. Senator PORTMAN. So when are we going to cover these people? Mr. LEWIS. One of the things we are examining is can we expand the capability of the system to handle that larger volume, and that is a work in progress and something that we could report back to you on” (*The Navy Yard Tragedy*, 2013, p. 37).
8. Problems with CE are not necessarily funding, but “It is a question of having the right criteria in place to conduct the evaluations and then what we do with the data once it is generated from the system, how you evaluate that and how you take action based on that information” (*The Navy Yard Tragedy*, 2013, p. 37).

9. "A number of pilot studies have been initiated to assess the feasibility of select automated records checks and the utility of publicly available electronic information, to include social media sites, in the personnel security process. Although these pilots have identified actionable information, they indicate that retrieving, analyzing, and processing the data is likely to be resource intensive. More research is required to assess resource impacts and determine the most effective method to utilize publically available electronic information while protecting the privacy and civil liberties of those individuals being evaluated" (*The Navy Yard Tragedy*, 2013, p. 65).
10. Although shortening the time for periodic reinvestigations would help identify issues, “it also adds significant cost and resource burdens to federal agencies and to the federal adjudicators” (*The Navy Yard Tragedy*, 2013, p. 100).
11. “But the larger issue is how do we collect—how do we identify and collect relevant information that allows us to constantly adjust our perspective about cleared individuals and individuals who are in trusted positions? And that is really the challenge” (*The Navy Yard Tragedy*, 2013, p. 169).
12. “I hate to keep blowing the same horn, but the continuous evaluation process of not just collecting the information but having the staff available to evaluate the information and take action on that information, to me that is the real issue here” (*The Navy Yard Tragedy*, 2013, p. 169).
13. “Moreover, with the proposed implementation of continuous evaluation, the workload of agencies’ security offices could significantly increase, making it critical for agencies to have a high-quality clearance revocation process in place.” (USGAO, 2014b, pp. 53-4).
14. “The Report explained that CE is an ambitious undertaking-- “Success of the CE program will depend on a fully-integrated solution across government, which will eliminate inefficiency and avoid the expenses of duplicative systems”--and the report also recognized the challenges and stated how much is yet to be done to reach that goal” (S. 113-283, 2014).
15. “Implementing a system for continuous evaluation is resource intensive, and poses genuine technical and procedural challenges” (S. 113-283, 2014).
16. “Currently there is no government-wide capability, plan or design present in the investigative community to operate a data-driven architecture to collect, store, and share relevant information” (S. 113-283, 2014).
17. “S. 1618 provides that random audits would not be required if more frequent automated checks of governmental and commercial records and data are being conducted with respect to the individual” (S. 113-283, 2014).
18. “This exemption for individuals who are the subject of more frequent automated checks is a key component of the program” (S. 113-283, 2014).

APPENDIX R

USE OF TERM “SURVEILLANCE”

Document	Number of times “surveillance” occurred	Context of the use of the term
1	6	“Surveillance used in reference to Snowden’s access to the NSA’s surveillance data
2	0	
3	0	
4	0	
5	0	
6	0	
7	0	
8	0	
9	0	
10	NOT INCLUDED IN STUDY	
11	0	
12	6	“Surveillance” used in reference to Snowden’s access to the NSA’s surveillance data
13	0	
14	0	
15	0	
16	0	
17	3	“Surveillance” used in reference to the need for OPM to be watched through audits for transparence
18	NOT INCLUDED IN STUDY	
19	0	
20	1	Facilities use a guard up front to carry out surveillance of those entering a building
21	NOT INCLUDED IN STUDY	
22	0	
23	0	
24	0	
25	1	“Surveillance” used in reference to Snowden’s access to the NSA’s surveillance data
26	0	
27	1	Some need clearance to work in surveillance field
28	0	
29	NOT INCLUDED IN STUDY	

APPENDIX S

LIST OF ARTICLES

1 *The Insider Threat to Homeland Security: Examining Our Nation's Security Clearance Process*. Hearing before the Subcommittee on Counterterrorism and Intelligence of the Committee on Homeland Security House of Representatives. 113th Cong. (2013). Retrieved from ProQuest Congressional Database.

2 S. 2683 - Clearance and Over-Classification Reform and Reduction Act. (2014). Retrieved from ProQuest Congressional Database.

3 H.R. 5240 - Clearance and Over-Classification Reform and Reduction Act. (2014). Retrieved from ProQuest Congressional Database.

4 *DC Navy Yard Shooting: Fixing the Security Clearance Process*. Hearing before the Committee on Oversight and Government Reform House of Representatives. 113th Cong. (2014). Retrieved from ProQuest Congressional Database.

5 113th Cong. Rec. H.R. 2860 (daily ed. January 14, 2014) (statement of Mr. Farenthold). Retrieved from ProQuest Congressional Database.

6 H.R. 490 - Security Clearance Accountability, Reform, and Enhancement Act of 2015. (2015). Retrieved from ProQuest Congressional Database.

7 H.R. 4022 - Security Clearance Accountability, Reform, and Enhancement Act of 2014. (2014). Retrieved from ProQuest Congressional Database.

8 Enhanced Security Clearance Act of 2013 Offered by Ms. Collins, 113th Cong. Rec. S1618 (daily ed. October 3, 2013). Retrieved from ProQuest Congressional Database.

9 S. 113-111 - Security Clearance Oversight and Reform Enhancement Act. (2013). Retrieved from ProQuest Congressional Database.

10 Not Included

11 S. 113-276 - Security Clearance Oversight and Reform Enhancement Act. (2014). Retrieved from ProQuest Congressional Database.

12 The Insider Threat to Homeland Security: Examining Our Nation's Security Clearance Process. Hearing before the Subcommittee on Counterterrorism and Intelligence of the Committee on Homeland Security House of Representatives. 113th Cong. (2013). Retrieved from ProQuest Congressional Database.

13 OPM IG Act, 113th Cong. Rec. H.R. 2860 (daily ed. January 14, 2014). Retrieved from ProQuest Congressional Database.

14 US Government Accountability Office. (2013). Security clearances: Additional mechanisms may aid federal tax-debt detection (Report No. GAO 13-733). Retrieved from ProQuest Congressional Database.

15 H. Rep. (2014). Committee on Oversight and Government Reform. Slipping through the cracks: How the D.C. Navy Yard shooting exposes flaws in the federal security clearance process. Retrieved from http://oversight.house.gov/wp-content/uploads/2014/02/Aaron-Alexis-Report-FINAL.pdf

16 S. 13-111 - Security Clearance Oversight and Reform Enhancement Act. (2013). Retrieved from ProQuest Congressional Database.

17 *Safeguarding Our Nation's Secrets: Examining the Security Clearance Process*. Joint Hearing before the Subcommittee on the Efficiency and Effectiveness of Federal Programs and the Federal Workforce and Subcommittee on Financial and Contracting Oversight of the Committee on Homeland Security and Governmental Affairs of the United States Senate. 113th Cong. (2013). Retrieved from ProQuest Congressional Database.

18 Not Included

19 S. 113-257 -Preventing Conflicts of Interest with Contractors Act. (2014). Retrieved from ProQuest Congressional Database.

20 *The Navy Yard Tragedy*. Hearing before the Committee on Homeland Security and Governmental Affairs of the United States Senate. 113th Cong. (2013). Retrieved from ProQuest Congressional Database.

21 Not Included

22 Nomination of Hon. Katherine Archuleta. Hearing before the Committee on Homeland Security and Governmental Affairs of the United States Senate. 113th Cong. (2013). Retrieved from ProQuest Congressional Database.

23 Government Accountability Office. (2014). Personnel security clearances: Additional guidance and oversight needed at DHS and DOD to ensure consistent application of revocation process. (Report No. GAO 14-640). Retrieved from ProQuest Congressional Database.

24 *Safeguarding Our Nation's Secrets: Examining the National Security Workforce*. Hearing before the Subcommittee on the Efficiency and Effectiveness of Federal Programs and the Federal Workforce of the Committee on Homeland Security and Governmental Affairs of the United States Senate. 113th Cong. (2013). Retrieved from ProQuest Congressional Database.

25 Government Accountability Office. (2014). Information security: Agencies need to improve oversight of contractor controls. (Report No. GAO 14-612). Retrieved from ProQuest Congressional Database.

26 S. 113-283 - Enhanced Security Clearance Act of 2014. (2014). Retrieved from ProQuest Congressional Database.

27 Congressional Research Service. (2014). The debate over selected presidential assistants and advisors: Appointment, accountability, and congressional oversight. (Report No. 40856). Retrieved from ProQuest Congressional Database.

28 *Facility Protection: Implications of the Navy Yard Shooting on National Security*. Hearing before the Subcommittee on Oversight and Management Efficiency of the Committee on Homeland Security of the United States House of Representatives. 113th Cong. (2013). Retrieved from ProQuest Congressional Database.

29 Not Included