Carnegie Mellon University
Software Engineering Institute

Data Analysis of Security Clearance Appeal Decisions

CERT National Insider Threat Center
Sarah E. Miller

Month and Year (date added at time of publication)

SPECIAL REPORT
CMU/SEI-2018-SR-XXX

Program Name

http://www.sei.cmu.edu

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM18-1306

Table of Contents

List of Figures

List of Tables

Acknowledgments

Executive Summary

Abstract

The decision-making process by which security clearance decisions are made is one that affects millions of employees and contractors working in the federal government and the defense industry. Unfortunately for applicants seeking a security clearance, and the organizations that sponsor them, any insights into this decision-making process are not validated or codified. For the Department of Defense (DoD) and other federal agencies, the issue of whom to trust with access to classified information is complicated by the complexity of each individual case and the potential for falsification(s) by applicants. This project seeks to use statistical methods by which the decision-making process can be codified. Best practices for applicants and sponsoring organizations will be developed in concordance with the results of these findings.

1 Introduction

As of 2014, approximately 5.1 million Americans held security clearances, costing several billion dollars in investigation costs (Fung, 2014). With the exception of changes to the actual security clearance application forms, the process for investigating security clearance applicants has largely remained unchanged since World War II (McGarvey, 2017). This investigative process is intended to identify the potential for an individual to violate trust, specifically in regards to the disclosure of classified information. In an increasingly digital world, the possibility of disclosure becomes greater and the potentially outdated, expensive investigative process make the stakes for granting clearances that much higher. In general, there is not much information on how to get a clearance that is codified or based on more than anecdote, but it is a topic of growing concern. To provide quantifiable insight into this process, this project seeks to use publicly available case information on industrial security appeal decisions to demystify the decision-making process behind granting clearances using behavioral models for insider threat and espionage as a frame for interpreting results. References to these sources are available online as seen in on the Department of Defense Office of Hearings and Appeals repository (Defense Office of Hearing and Appeals, 2018). Each case is judged in accordance with thirteen Adjudicative Guidelines[1], which are described in Table 1below.

Table 1: Adjudicative Guidelines

Letter	Adjudicative Guideline	Brief Description
A	Allegiance to the United States	Participation in or supporting acts against the United States or those that can compromise national security
B	Foreign Influence	Foreign contracts and interests (e.g., business, financial, and property interests) that could result in divided allegiance
C	Foreign Preference	Preference for a foreign country over the United States
D	Sexual Behavior	Sexual behavior that involves a criminal offense, reflects a lack of judgement or discretion, or otherwise makes an individual subject to coercion, exploitation, or duress
E	Personal Conduct	Conduct involving questionable judgment, lack of candor, dishonesty, or unwillingness to comply with rules and regulations
F	Financial Considerations	Failure to live within one's means, satisfy debts, and meet financial obligations
G	Alcohol Consumption	Excessive alcohol consumption
H	Drug Involvement	Illegal use of controlled substances, including misuse of prescription and non-prescription drugs
I	Psychological Conditions[2]	Certain emotional, mental, and personality conditions that can impair judgment, reliability, or trustworthiness, with or without a formal diagnosis of a disorder
J	Criminal Conduct	Criminal activity, inclusive of minor offenses, evidence of criminal conduct, or discharge / dismissal from the Armed Forces for other than "Honorable" reasons
K	Handling Protected Information	Deliberate or negligent failure to comply with rules and regulations for handling protected information (e.g., classified and other sensitive government information or proprietary information), including disclosure to unauthorized persons

[1] The full text of the Adjudicative Guidelines can be found online at: http://ogc.osd.mil/doha/SEAD4_20170608.pdf

[2] Mental health counseling in and of itself does not disqualify an individual for access to classified information.

Letter	Adjudicative Guideline	Brief Description
L	Outside Activities	Certain types of additional / outside employment that poses a conflict of interest with an individual's security responsibilities, especially if it creates an increased risk for unauthorized disclosure
M	Use of Information Technology Systems	Failure to comply with rules, procedures, guidelines, or regulations pertaining to information technology systems

Although we do not discuss in this report why the Adjudicative Guidelines reflect concerning behavior for those seeking access to classified information, the context and justification for these guidelines, including concerning conditions, are discussed in official documentation.

1.1 Insider Threat

The most recent definition of insider threat published by CERT refers to insider threat as "the potential for an individual who has or had authorized access to an organization's assets to use their access, either maliciously or unintentionally, to act in a way that could negatively affect the organization" (Costa, CERT Definition of 'Insider Threat' - Updated, 2017). In the context of a workplace, this could take many forms, from the cyber to the physical / kinetic. Prediction of these incidents would necessarily be paramount to the defense industry and in turn a security investigator.

A model for predicting insider threat, known as the CERT Critical Path to Insider Threat, developed via the collaboration of CERT and then visiting scientist Dr. Eric Shaw in 2006, is one frame that can be used (Shaw & Sellers, 2015). From Personal Predispositions to Problematic Organizational Responses, the CERT Critical Path to Insider Threat accounts for several dimensions for measuring events that precipitate insider threat. The general concept of the Critical Path is that any individual inherently has their own Personal Predispositions, but as they move along the path, the greater the risk that person poses for committing a Hostile Act, i.e., becoming a full-blown insider threat. Within the context of the clearance decisions, information should be available on Personal Predispositions, Stressors, and Concerning Behaviors, if based solely on the adjudicative factors used in each case. It is less likely the appeals related to specific applicants will address Problematic Organizational Responses, unless in specific circumstances where it may be seen as a mitigating factor for undesirable behavior(s). In some instances, there may even be a Hostile Act that is captured, as guidelines K through M reflect problematic workplace activities. One of the assumptions of the model is that prior maladaptive behavior will be predictive of future maladaptive behavior, i.e., if an individual has already engaged in some hostile insider act(s), then we assume they are more likely to engage in those or similar behavior(s) in the future. To that end, it will be important to identify the extent to which individuals with hostile acts in their investigative record are (or are not) granted clearances upon appeal.

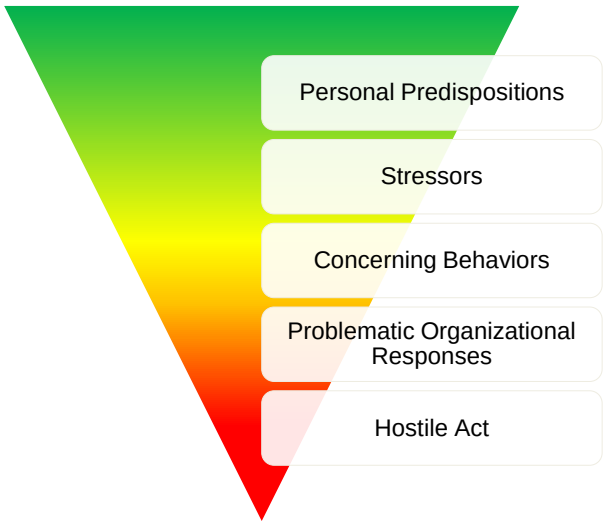

Figure 1: CERT Critical Path to Insider Threat

These "hostile acts" can be categorized through a number of dimensions or means. For the purposes of this project, the taxonomy offered by Casey (2015) will be used to help frame, capture, and categorize any confirmed incidents of insider threat found in the industrial security clearance decision corpus. These categories are as follows:

- Accidental Leak
- Misuse
- Fraud
- Physical Theft
- Violence
- Sabotage
- Product Alteration
- Opportunistic Data Theft
- Espionage

While these categories are useful, they may not fully capture the nuances of each incident, so additional categories may be added to build a fuller taxonomy. Furthermore, in keeping with the intent of the updated CERT definition for insider threat, "Violence" will be inclusive of sexual harassment.

1.2 Domestic Violence

Along those same lines, this project seeks to capture data on domestic violence. Though not necessarily a workplace crime, domestic abusers holding a security clearance is a concern for many domestic violence victims and the defense community, as evidenced by an update to the SF-86 Questionnaire for National Security Positions in 2010 to specifically request information on domestic violence (Gibson, 2014). Furthermore, some workplace active shooters were shown to have a background of committing domestic abuse (Gibson, 2014). Within the context of both the clearance process and insider threat, domestic violence incidents are relevant.

1.3 Espionage

While the taxonomy used by Casey (2015) does mention espionage, it is worthwhile to explore how behavioral frameworks for espionage may differ. After all, espionage is not simple disclosure, but treason – a betrayal of not just trust, but country. Burkett (2013) describes the traditional MICE framework for understanding a spy's motives: Money, Ideology, Compromise or Coercion, and Ego or Excitement. In putting motivation in simpler terms, it is all the more clear how these motivations may manifest in behaviors. In turn, these behaviors may be reflected in adjudicative guidelines.

Table 2: Insider Threat Model Mapping to Relevant SF-86 Questionnaire Sections provides a mapping for each adjudicative guideline with the Critical Path and MICE models, which are related to specific sections of the SF-86. The information used in each clearance appeal has a connection and provenance; each of these appeals can be traced back to when each applicant first completed their security clearance application. Each appeals case decision is as close of an artifact that is available relative to these applications, or even the investigator's notes in each case.

Table 2: Insider Threat Model Mapping to Relevant SF-86 Questionnaire Sections

Section #	Information	Critical Path	MICE
1 – 8	Contact, DOB	N/A	N/A
9	Citizenship	N/A	Ideology
10	Multiple Citizenships Foreign Passport(s)	Personal Predispositions Concerning Behaviors	Ideology Compromise / Coercion
11	Residence History	N/A	N/A
12	Education	N/A	N/A
13	Employment History	Stressors Concerning Behaviors Hostile Acts	N/A
14	Selective Service Record	N/A	N/A
15	Military History	Stressors	Excitement
16	3 References	N/A	N/A
17	Marital Status	Stressors	Coercion
18	Relatives	Stressors	Coercion
19	Foreign Contacts	Concerning Behaviors	Compromise
20	Foreign Activities	Concerning Behaviors	Compromise
21	Mental Health	Personal Predispositions	Compromise
22	Police Record	Concerning Behaviors	Excitement
23	Illegal Drugs / Drug Activity	Concerning Behaviors	Compromise Excitement
24	Use of Alcohol	Concerning Behaviors	Compromise Excitement
25	Investigations and Clearance History	Concerning Behaviors	Compromise
26	Financial Record	Stressors	Money
27	Use of IT Systems	Concerning Behaviors Hostile Acts	Ego
28	Non-Criminal Court Actions	Stressors	Money
29	Association Record	Personal Predispositions Concerning Behaviors	Ideology

2 Research Questions

The following research questions informed the methodology and analysis associated with this project:

1. What is the ratio of affirmed clearance denials to approvals granted upon appeal?
2. What adjudicating factors, if any, are significantly correlated (either positively or negatively) with each other?
    a. What new insights, if any, can be gleaned by these relationships?
    b. What emergent features related to one or more adjudicating factors?
3. What hostile insider acts, if any, can be identified?
    a. How are these related to other adjudicating factors?
4. What is the impact of falsifications on the SF-86 on appeal outcomes?
    a. Is there a statistically significant correlation or causal relationship that can be quantified?
5. Are there best practices or guidance for industrial security practitioners, clearance applicants, and appellants that can be abstracted beyond the thirteen adjudicative guidelines?

3 Methodology

The methodology for this project was focused on designing and implementing a database of the Industrial Security Clearance Decisions, particularly adjudicative guidelines and behavioral information presented in each case. The cases ranged in date from November 1996 (the oldest on record) to December 2016.

3.1 Web Scraping

Using publicly available web browser extension, case features were extracted by feature from the web page corresponding to each year of decisions. The text was then organized into .csv workbooks, with a column corresponding to each feature. The features are described below.

3.1.1 Case Features

- *Case Number*: The case number is in the form of a two digit number, the last two digits of the year in which the case was heard, typically followed by a four digit number, the order in which that case appeared before DOHA in that given year. These digits are followed by a ".a" or ".h," with ".a" corresponding to an Appeal Board and ".h" corresponding to a Hearing Board case. While the specifics of each component of the case number are less important to the overall analysis, they served as unique identifiers for the case for de-duplication in the database structure.
- *Keywords*: The keywords presented for each case correspond to the adjudicative guidelines, using either a variation on the guideline's name, or the guideline's letter. In a small number of instances, anomalous keywords were used.
- *Date of Appeal*: The date of appeal is when a decision was entered by the adjudicative judge for the case.
- *Digest*: Given the tag "Digest" in the HTML of the pages, this text features a judgment summary which includes the outcome.

A small subset of the more recent appeals included cases not related to security clearance investigations themselves. These cases were identified so that they could be isolated from analyses.

- "*Deception*," specifically that an applicant falsified material facts on a Declaration for Federal employment form (306).
- "*Common Access Card (CAC),*" meaning that an applicant was seeking a standard identification card issued by the Department of Defense.
- "*Security Violations*," which included workplace offenses that were similar to those described in Guideline K: Handling Protected Information and Guideline M: Use of Information Technology Systems adjudicative guidelines.

Aside from the case features, each case had a corresponding file. Using a Python script, URLs for the individual case files were found. After filtering for only those URLs that ended in ".pdf," these links were saved into a .csv file. Again, using publicly available web browser extension, this .csv file was imported and 3,157 case file PDFs were downloaded.

- *Case File*: With the exception of 55 cases that are missing information and have broken links, the full-body text of the appeal decision is available. For cases from between 1996 and 2000, this case file is HTML. For cases from 2001 and to the present, they are available in PDF format. Each PDF case file was named using the case number for reference.

3.2 Importing the Data

Once each year's worth of data was copied and saved into .csv sheets, these sheets were appended into a relational database instance. Once each year was imported and the cases were de-duplicated, 20,514 unique cases were reviewed and prepared for further feature identification.

3.3 Tagging the Data

After importing the .csv files into a database, and once gender was confirmed in each case, additional features were made into new columns and fields. With the exceptions of Age (numerical) and Insider Threat (categorical), all additional features were binary. Many of these features were added iteratively after encountering more cases and identifying emergent features.

3.3.1 Demographic Features

- *Previous or Current Clearance*: Applicants that were known to have previously, or currently, be holding a security clearance.
- *Traumatic Life Event*: Stressors beyond the applicant's control, including nationwide crises affecting the applicant, severe health conditions, loss of a close family member, being the victim of a crime, or unexpectedly taking care of a family member (such as in the case of severe illness) that may be perceived as mitigating factors for any concerning behaviors.
- *Former / Current Military or Law Enforcement*: Applicants that served or were serving as active duty in the U.S. military or, in only a minority of instances, law enforcement.

3.3.2 Concerning Behaviors

- *Falsification(s)*: Falsifications were identified in a subset of 5,043 cases by selecting one of three binary options: No Falsification Alleged, Known Falsification, or Rebutted Falsification Allegation. These falsifications would be limited in scope to those made on a security clearance application or in an interview with an investigator. Known Falsifications are further limited to those intentional in nature.
- *Caused Death*: Applicants that committed offenses that caused the death of another. These crimes may include manslaughter or vehicular homicide. This concerning behavior was intended as a sub-feature of Adjudicative Guideline J: Criminal Conduct.
- *Domestic Violence*: Applicants that were known to commit domestic violence, without the limitation of a convictions. Applicants that were victims of domestic violence would not be included in this category, but instead under traumatic life events. This concerning behavior was intended as a sub-feature of Adjudicative Guideline J: Criminal Conduct.
- *Child Sexual Abuse*: Applicants that were known to have committed sexual abuse against minors, which is inclusive of statutory rape, without the limitation of a conviction. This concerning behavior was intended as a sub-feature of Adjudicative Guidelines D, E, and J.

- *Child Pornography*: Applicants that knowingly viewed and / or downloaded child pornography. This concerning behavior was intended as a sub-feature of Adjudicative Guidelines D, E, and J.
- *Sex Work*: Applicants that paid, or were paid (in only one case), for sex work, i.e., solicitation or prostitution. This concerning behavior was intended as a sub-feature of Adjudicative Guidelines D, E, and J.

4 Data Analysis

4.1 Summary Statistics (Frequency)

Overall, the appeals process was largely unfavorable to applicants: 13,623 applicants (68%) were denied a clearance on appeal, while only 6,112 applicants (31%) were granted a clearance. In the remaining 1-percent of cases, the outcome was unknown because the case was remanded, the applicant died, the applicant withdrew their appeal, or, in 55 cases, the data was simply missing. The decisions by outcome by year can be seen in Figure 2, where "Against" and "For" represent "Denied" and "Granted." Note that there is an uptick in the total number of cases post-2001, and therefore post-9/11.

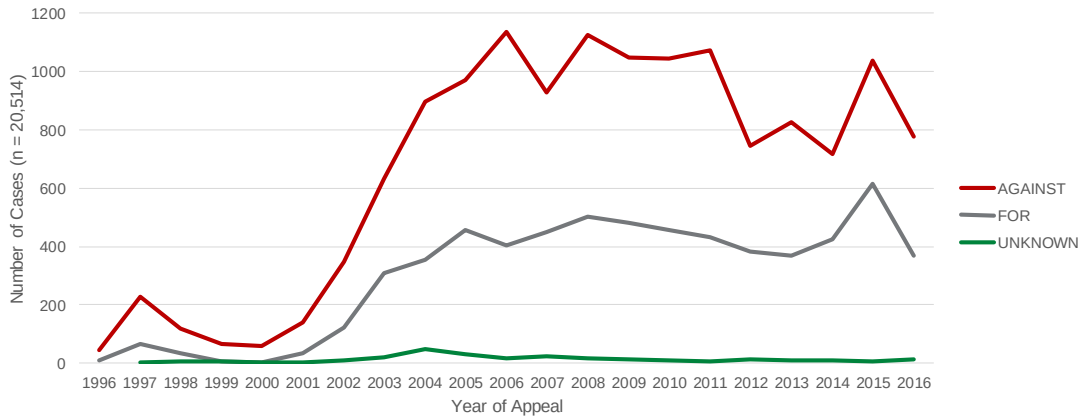

Figure 2: Security Clearance Appeal Decisions over Time

None of the 20,514 total cases entered for appeal involved a violation of Guideline A, Allegiance to the U.S.A. and for that reason it is not included in the frequency table below. Percentage counts are taken out of the total number of cases, not the total frequency of all guidelines cited. The guidelines that pose the greatest likelihood of indicating insider involvement, Guidelines K through M (Handling Protected Information, Outside Activities, and Use of Information Technology Systems), only amount to roughly 1-percent of all cases.

Table 3: Adjudicative Guideline Frequency in Security Clearance Appeal Decisions

Letter	Adjudicative Guideline	Count	Percentage
B	Foreign Influence	3526	17.2
C	Foreign Preference	1632	8.0
D	Sexual Behavior	483	2.4
E	Personal Conduct	7344	35.8
F	Financial Considerations	10720	52.3
G	Alcohol Consumption	1865	9.1
H	Drug Involvement	2211	10.8
I	Psychological Conditions	71	0.3
J	Criminal Conduct	3714	18.1
K	Handling Protected Information	59	0.3
L	Outside Activities	58	0.3

Letter	Adjudicative Guideline	Count	Percentage
M	Use of Information Technology Systems	52	0.3

For 2,856 applicants with Foreign Influence and / or Preference concerns, a country of concern was identified. For 383 of these individuals (13.4%), multiple countries of concern were identified. Focusing only on individuals that listed one country of concern, outcomes were determined by country. Although tabulating the total number of instances for each country is possible, determining in a methodical way to what extent a given outcome would be related to one or more of the countries of concern was outside the scope of this project. The case files reveal, as is evidenced in Table 4: Security Clearance Appeal Decisions by Country of Concern, that countries with known active intelligence against the U.S. were more associated with clearance denials than countries known to assist in the U.S. in efforts to combat global terrorism (Coats, 2017). Although such preferences may not come into play for the individual with said ties, these circumstances are inherently challenging for adjudicative judges to weigh. Ultimately these judges must be somewhat conservative in finding in favor for the interests of national security, which these outcomes frequencies related to each country bear out.

Table 4: Security Clearance Appeal Decisions by Country of Concern

Country	Granted	Denied	Total
Iran	99 (35.6%)	179 (64.4%)	**278**
China	100 (36.9%)	171 (63.1%)	**271**
Taiwan*	160 (69.3%)	71 (30.7%)	**231**
Israel*	86 (53.4%)	75 (46.6%)	**161**
India*	107 (76.4%)	33 (23.6%)	**140**
Afghanistan*	70 (51.1%)	67 (48.9%)	**137**
Russia	36 (33.6%)	71 (66.4%)	**107**
Vietnam*	64 (74.4%)	22 (25.6%)	**86**
Lebanon	35 (47.9%)	38 (52.1%)	**73**
Pakistan	27 (37.0%)	46 (63.0%)	**73**
South Korea*	40 (64.5%)	22 (35.5%)	**62**
Nigeria*	34 (65.4%)	18 (34.6%)	**52**
United Kingdom*	31 (60.8%)	20 (39.2%)	**51**
Iraq*	34 (73.9%)	12 (26.1%)	**46**
Egypt*	20 (51.3%)	19 (48.7%)	**39**
Jordan*	24 (66.7%)	12 (33.3%)	**36**
Turkey	17 (50.0%)	17 (50.0%)	**34**
Canada*	22 (68.8%)	10 (31.3%)	**32**
Colombia*	23 (82.1%)	5 (17.9%)	**28**
Germany	11 (44.0%)	14 (56.0%)	**25**

* More than half of the cited instances resulted in a clearance for the applicant.

Of course, there are more than adjudicative factors to consider in understanding the data. Women represented a minority of applicants, which may be reflective of the overall defense industry. However, many of these women were actually seeking position eligibility, i.e., they filled out an SF-85P and were seeking a position of trust, not necessarily a security clearance. Only 1-percent of applicants that filed appeals were ineligible for a clearance via the Smith Amendment, also known as 10 U.S.C. §986, wherein the Department of Defense cannot grant a security clearance to

an individual who spent more than 12-months in prison. While waivers of the Smith Amendment are possible, they require approval from the Secretary of Defense.

Table 5: Demographic Features

Demographic Feature	Count	Percentage
Female	4215	20.5
Previous Clearance	566	2.8
Traumatic Life Event	376	1.8
Former / Current Military or Law Enforcement	635	3.1
Smith Amendment	197	1.0
Position Eligibility	510	2.5

Applicant age was identified in a sample of 3,863 cases (18.8%). Applicants ranged in age from 19 to 82, though the middle 50-percent of applicants were between 34 and 51 years old. Both the average and median range was approximately 43 years old. Though there was an applicant aged 82 years old, she was technically a statistical outlier. A box-and-whisker plot of their ages can be seen below.

Figure 3: Age Distribution of Appellants

When grouping these applicants into 5-year age ranges, older applicants appear to be more likely to obtain a clearance. Only applicants aged between 65 to 69 years old, or 70 years old or older, had more than a 50-perecent success rate in obtaining a clearance on appeal. There are two primary interpretations for this trend: Older applicants may be viewed as more trustworthy or they have more opportunity for more youthful indiscretions to be mitigated by time.

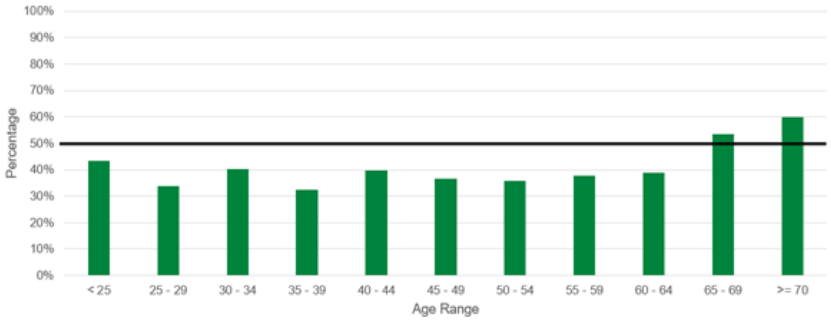

Figure 4: Positive Security Clearance Appeal Decisions by Appellant Age

All told, the concerning behaviors identified as sub-features of Criminal Conduct or Sexual Behavior did not make up more than 1-percent of applicants each. Security Violations, an anomalous keyword that could be associated with insider threat, also only accounted for less than 1-percent of applicants.

Table 6: Frequency of Identified Concerning Behaviors

Concerning Behavior	Frequency	Percentage
Domestic Violence	130	0.6
Caused Death	20	0.1
Child Sexual Abuse	95	0.5
Child Pornography	38	0.2
Solicitation / Prostitution	64	0.3
Security Violations	141	0.7

At least 420 individuals were included in this sample of insider threat observables, or hostile acts. The total frequency of each category is inclusive of the separate acts committed by each insider, with some insider committing multiple acts. The percentage per category is taken out of the total number of insiders, not the total frequency of hostile acts. Overall, approximately 46-percent of hostile acts fell within the definitions of the [Casey 2015] taxonomy. None of the instances of insider threat were classified as accidental leak, as there did not seem to be actual leaks as a result of any known negligence. Furthermore, while two instances fit within the taxonomy definition of espionage, this was related to what might be considered within the context of industrial espionage and not the legal definition of national security espionage.

Table 7: Frequency of Insider Threat Observables Using the Casey (2015) Taxonomy

Category	Frequency	Percentage
Misuse	182	43.3
Fraud	110	26.2
Violence	36	8.6
Physical Theft	24	5.7
Opportunistic Data Theft	14	3.3
Sabotage	12	2.9
Product Alteration	3	0.7
Espionage	2	0.5

Again, not all of the nuances of each insider incident was fully captured by the previous taxonomy. Based on the insider acts themselves, new trends were identified, affinity grouped, and arranged into a supplementary taxonomy.

Table 8: Insider Threat Observables Using Emergent Taxonomy

Category	Frequency	Percentage
Substance / Alcohol Use at Work	103	24.5

Category	Frequency	Percentage
Military Incidents	94	22.4
Concerning Workplace Behaviors	74	17.6
Falsifications	59	14.0
Security Violations	39	9.3
Failure to Report or Act	23	5.5
Non-Malicious / Negligence	23	5.5
Clearance History	11	2.6
Social Network Risks	11	2.6
Hacking Activity	10	2.4
Physical Security Violations	8	1.9

Although 59 instances of falsifications to employers were identified as insider threats, a sample of 5,043 incidents were tagged for falsifications on security clearance applications or to investigators. Of this sample, 56-percent included known falsification, 35-percent involved no allegation of falsification, and only 9-percent successfully rebutted an accusation of intentional falsification. While this sample is not necessarily representative of all 20,514 cases, they serve to highlight the prevalence of falsification on the SF-86 (which is a federal offense that can result in up to five years in prison).

4.2 Correlational Statistics

Correlational and binary logistic regression was performed using SPSS. Outcome was coded as "0" for clearance denied and "1" for clearance granted. Adjudicating factors and associated subfeatures were coded as binary (1 for "present", 0 for "absent"). Negative correlations were interpreted as meaning that a particular guidelines was more difficult to mitigate, or that the presence of the concern had a negative impact on obtaining a clearance. Conversely, a positive correlation suggested that concerns were less difficult to mitigate.

Correlations for Alcohol Consumption, Psychological Conditions, Handling Protected Information, Outside Activities, and Use of Information Technology Systems were not significant. With the exception of Alcohol Consumption, these adjudicative guidelines were used in only a small portion of cases, so there simply may not be enough data to determine significant correlation.

Table 9: Correlation between Adjudicative Guidelines and Outcome

Adjudicative Guideline	Pearson Coefficient (r)
Foreign Influence	-.076[b]
Foreign Preference	.055[b]
Sexual Behavior	-.039[b]
Personal Conduct	-.314[b]
Financial Considerations	.045[b]
Alcohol Consumption	-.023

Adjudicative Guideline	Pearson Coefficient (r)
Drug Involvement	-.089[b]
Psychological Conditions	-.003
Criminal Conduct	-.172[b]
Handling Protect Information	.010
Outside Activities	.011
Use of Information Technology Systems	.020

[a.] Significant at the 0.05 level (2-tailed).
[b.] Significant at the 0.01 level (2-tailed).

Female applicants were less likely to have: concerning sexual behaviors, alcohol abuse or dependence, issues with drugs, a criminal history, committed domestic violence, previously served in the military, or have committed child sexual abuse. Female applicants were more likely than male applicants to have financial concerns or experienced a traumatic life event. Female applicants were more likely than male applicants to obtain a clearance on appeal. While it is not necessarily "being female" that makes it easier to obtain a clearance, they were not associated with some of the harder-to-mitigate adjudicative guidelines. Since the primary concern with female applicants appeared to be financial, which was more easily mitigated, it follows that they were more successful on appeal than male applicants.

Table 10: Significant Correlations Involving Female Applicants

Significant Correlations Involving Female Applicants	
Feature	*Pearson Coefficient (r)*
Sexual Behavior	-.068[b]
Financial Considerations	.173[b]
Alcohol Consumption	-.092[b]
Drug Involvement	-.060[b]
Criminal Conduct	-.088[b]
Domestic Violence	-.045[b]
Previous Clearance	-.032[a]
Traumatic Life Event	.075[b]
Child Sexual Abuse	-.029[a]
Former / Current Military	-.040[b]
Outcome (Granted Clearance)	.068[b]

[a.] Significant at the 0.05 level (2-tailed).
[b.] Significant at the 0.01 level (2-tailed).

Applicants with a military (or law enforcement) background were less likely to have used drugs or have foreign preference concerns. On the other hand, they were more likely to correlate with a number of concerning behaviors. However, military applicants were more likely to obtain a clearance on appeal. Since it is already been established that female applicants were less likely to be military applicants (and therefore vice versa), positive outcomes for military applicants are likely not related to the applicants themselves being women.

Table 11: Significant Correlations Involving Military Applicants

Feature	Pearson Coefficient (r)
Criminal Conduct	.029[a]
Domestic Violence	.031[a]
Drugs	-.040[b]
Foreign Preference	-.029[a]
Caused Death	.045[b]
Child Sexual Abuse	.039[b]
Previous Clearance	.118[b]
Outcome (Granted Clearance)	.048[b]

[a.] Significant at the 0.05 level (2-tailed).
[b.] Significant at the 0.01 level (2-tailed).

As it has already been established, domestic violence is significantly negatively correlated with female applicants, but significantly positively correlated with military applicants. However, additional correlations were identified as being worthy of note. Domestic violence has a significant positive correlation with criminal conduct, but likely merely acts as a sub-feature of criminal conduct. Domestic violence is significantly less likely to co-occur with drug involvement or financial considerations, which may run counter to notions of domestic violence being synonymous with family dysfunction or financial distress. Domestic violence does not have a significant correlation with alcohol consumption or case outcome. However, alcohol consumption does not have a significant relationship with outcome either, so it is unclear if there are simply not enough incidents in the sample.

Table 12: Correlations Related to Domestic Violence

Feature	Pearson Coefficient (r)
Alcohol Consumption	.027
Criminal Conduct	.114[b]
Drug Involvement	-.029[a]
Financial Considerations	-.054[b]
Outcome (Granted Clearance)	.008

[a.] Significant at the 0.05 level (2-tailed).
[b.] Significant at the 0.01 level (2-tailed).

By looking at significant correlations, in either direction, that are related to one or all of the features associated with insider threat, we can begin to identify potentially "co-morbid" behaviors that could signal such insider activity. Adjudicative guidelines like Criminal Conduct, Drug Involvement, Financial Considerations, and Personal Conduct being negatively correlated with one or more of these insider threat features suggest that insider threats might not be signaled by these more outward or easily identified concerning behaviors. However, the significant positive correlations between Security Violations and Outside Activities suggest that conflicts of interest are associated with insider activity within the sample. The positive correlation between Use of Information Technology Systems and Handling Protected Information suggests that these insider

activities co-occur, so the presence of one may serve as a rationale for investigating for the possibility of the other.

Table 13: Insider Threat Features Matrix (Correlations for Insider Threat Activity)

	Use of Information Technology Systems	Security Violations	Handling Protected Information
Criminal Conduct	-.032[b]	-.040[b]	-.036[a]
Drug Involvement	-.025	-.032[a]	-.023
Financial Considerations	-.050[b]	-.062[b]	-.045[b]
Personal Conduct	-.032[a]	-.019	-.026
Outside Activities	-.002	.051[b]	-.002
Handling Protected Information	.414[b]	-.004	1

[a.] Significant at the 0.05 level (2-tailed).
[b.] Significant at the 0.01 level (2-tailed).

Beyond insider threat concerns, falsification concerns still persist. Again, any statistics related to falsifications pertain to only a sample of all cases. Falsifications largely act as a sub-feature of Personal Conduct, as evidenced by the correlation seen in Table XIII. Other adjudicative guidelines, like Criminal Conduct or Drug Involvement, being associated with falsification is understood as those concerns that are falsified the most. Falsifications are also associated with sex work, having been through the clearance process before, and failure to obtain a clearance. Regression analysis can reveal the extent to which an association between falsification and a negative outcome is causal.

Table 14: Correlations Related to Falsifications

Feature	Pearson Coefficient (r)
Criminal Conduct	.027
Drug Involvement	.130[b]
Personal Conduct	.771[b]
Sex Work	.032[a]
Previous Clearance	.093[b]
Outcome (Granted Clearance)	-.422[b]

[a.] Significant at the 0.05 level (2-tailed).
[b.] Significant at the 0.01 level (2-tailed).

4.3 Binary Logistic Regression

Binary logistic regression analyses were performed on a sample of 5,043 cases (24.6%). In this sample, outcome was known: clearance granted (coded as "1") or denied (coded as "0"). In the sample, 77.5-percent of cases resulted in a denied clearance, which is admittedly greater than that of the entire sample. The sample was chosen to highlight the impact of falsification on outcome. Falsification was entered as a categorical covariate with outcome as a binary dependent variable.

On its own, falsification is a significant predictor at $p < .001$ of the appeal outcome such that a known falsification is associated with a negative outcome (i.e., denied clearance) and a lack of known falsification is associated with a positive outcome (i.e., granted clearance).

Table 15: Binary Logistic Regression for Falsification and Security Clearance Appeal Outcome

Variables in the Equation						
Step 1[a]	*B*	*S.E.*	*Wald*	*Df*	*Sig.*	*Exp(B)*
Known Falsification			849.639	2	.000	
No Falsification Alleged	2.592		688.699	1	.000	13.351
Rebutted Falsification Allegation	3.249		662.413	1	.000	25.769
Constant	-2.937	.086	1171.444	1	.000	.053

[a.] Variable(s) entered on step 1: Falsification.

Although it is possible to add adjudicative guidelines to the model, it would not necessarily add to understanding of the appeals decision-making process as a whole. Although Personal Conduct or Criminal Conduct could be significant predictors, these factors could be duplicative of the established impact of falsifications and the Smith Amendment. Given the correlations provided on adjudicative guidelines and outcome, there is not necessarily a need to perform more regression analyses related to falsifications.

5 Conclusions and Recommendations

5.1 Advocating for Employee Assistance Programs

Since the early 1990's, the intelligence community has known from Project SLAMMER – wherein convicted spies were interrogated and asked "how they got away with it" – that "Heavy drinking, drug dependence, signs of depression or stress, extramarital affairs and divorce could be warning signs of a security problem" (Stein, 1994). However, not every supervisor, coworker, or even facility security officer will know how to deal with an employee's interpersonal issues becoming present in the workplace. Instead, in order to reduce uncertainty about how to respond, these potential insiders and spies should be formally referred to Employee Assistance Programs (EAPs). Adverse behavioral changes in employees are more manageable for employers when an EAP is in place.

Furthermore, EAPs can provide needed connections to communities of support that could improve their chances of obtaining a clearance. For employees with drug or alcohol abuse issues, at least 12 months, or ideally 24 months or more, of abstinence is recommended and connections to counselors and support groups can assist in those efforts. Likewise, employer-sponsored financial awareness or credit counseling programs have potential for mitigating financial consideration concerns.

5.2 Encouraging Honesty in Employees

Well-meaning facility security officers, or perhaps even lawyers, may encourage applicants for a clearance to withhold potentially damaging information to the detriment of the applicant. Although this may not always present an insurmountable obstacle to obtaining a security clearance, verifiable omissions reflect poorly on the applicant. Applicants may be able to mitigate some negative background details through the passage of time, but then fail to obtain a clearance because of an attempt to conceal that behavior. If applicants realize a mistake in their application, or rethink an omission, they should inform their employer's facility security staff, or potentially their federal sponsor, and withdraw before resubmitting a corrected application. If it is too late for an application to be withdrawn, applicants should admit or reveal their omission or falsification before a confrontation with DSS or OPM investigators. If the correlations and results of the binary logistic regression related to falsifications within the sample data hold for the entire population, then there is empirical evidence that lying is the "worst thing" that an applicant can do.

5.3 Mitigating Foreign Ties and Influence

Applicants should consider relocating or selling foreign assets or properties, though maintaining a vacation home in a foreign country may not always be viewed as a "red flag." Applicants should help their romantic partners seek legal citizenship status when necessary and possible. Applicants with dual-citizenship may want to consider their own willingness and desire to surrender foreign passports or formally renouncing other citizenship. Applicants may want to avoid sending money to relatives overseas whenever possible. Associations with countries known to engage in active intelligence collection (i.e., People's Republic of China, Germany) pose a particular challenge for

applicants and should be avoided or contextualized as much as possible. However, specific countries of concern may change over time.

5.4 Helping Military Applicants with Financial Concerns

While no significant correlation exists between the Military and Financial Considerations within the sample, in the overall case population, 306 of 635 appellants with a military background (48%) had financial concerns. At least 23 service members relied on their wives to handle their finances while deployed, which their wives in turn mismanaged or misused. Another five former servicemen struggled with finances in the transition back to civilian life, with at least two more military personnel the victim of identity theft while deployed. (It could be argued that three service members were victims of identity theft. In one additional instance, a 21-year-old soldier's mother opened credit cards in his name.) In addition to providing more financial counseling to those serving, those programs should be made available to military families as well.

5.5 Addressing Misconceptions and Developing Awareness around Domestic Violence

Approximately 29% of applicants that committed domestic violence were granted a clearance, which is in keeping with the trend in the overall sample. However, applicants with a military background account for 3% of all cases, but 8.5% of incidents of domestic violence. Ergo, military applicants are over-represented in instances of domestic violence. Domestic violence in these scenarios could be indicative of undiagnosed combat stress or post-traumatic stress disorder (Lawrence, 2016). The Bureau of Labor Statistics (2016) identified 500 incidents of workplace homicides in 2016, with coworkers or work associates responsible for killing approximately 13 women and 53 men, with "relatives or domestic partners [as] the most frequent assailant in work-related homicides involving women." Not only does employee-on-employee violence impact organizations, but the violence perpetrated by an employee's former or current partner. If we want to help employees keep their clearances and keep the workforce safe, then warning signs for being the perpetrator (or victim) of domestic violence should be incorporated into facility security programs and EAPs to help prevent violence from escalating.

5.6 Interpreting Clearance Appeal Results for Insider Threats

Applicants that had acted as insiders, albeit non-maliciously, were occasionally granted clearances. However, this should not be seen as a reason for ignoring such histories. Likewise, public concern over the background of individuals granted clearances, should they be made known, could negatively impact the reputation of sponsoring employers. Beyond concerns over ability to obtain a clearance, employers should consider how an employee fits into the culture and public image of their organization.

5.7 Limitations

Correlational analyses were conducted on a small sample of appealed cases, which may or may not reflect every applicant who is denied a clearance, let alone every applicant that applied for a clearance (and particularly not those who are granted a clearance). Since the majority of the case data was tagged manually, there is certainly room for human error.

6 Suggestions for Future Work

6.1 Using the Existing Data

Beyond the frequency and statistical analysis already performed on the existing data set collected, additional opportunities exist to understand the clearance appeals process and, perhaps by extension, the clearance adjudication process. For instance, the saved case decisions present a bounty of data for text analysis. Analysis of the decisions relative to the specific judges writing the appeal could reveal potential biases held by a judge or judges; in particular, analysis could potentially reveal biases held against specific adjudicative judges. With the appropriate entity-identification in place, it may also be possible to identify when it is the investigator, and not the judge, whose judgment is in question.

Implementation of Natural Language Processing (NLP) and Machine Learning (ML) algorithms with exception handling to automate the coding process could be useful to validate tagging, automate untagged cases, and analyzing new cases as they are added over time. For instance, the sample of roughly 5,000 cases (25%) could serve as a training set for identifying falsification(s) in new cases. Identifying another sample of test cases could be useful for time series analyses with ML, specifically matching behaviors to sequences of events along the Critical Path, or identifying trends in what constitutes enough (or not enough) time to mitigate an offense. Testing and evaluation of the accuracy of statistics, and the ML algorithm(s), over time as new data is introduced present a more long-term opportunity.

6.1.1 Extrapolation of a Normal Population

Arguably, we could attempt to extrapolate what a "normal" distribution may look like based on cases where appellants were ultimately granted a clearance in order to develop baseline frequencies of concerning behaviors within the thirteen Adjudicative Guidelines. The appeal cases reviewed in this process represent a "self-selecting" subpopulation within the 2.5-percent of clearances that are denied, in general, per year. (While these 2.5-percent of applicants denied are not comparable to general population, they are from a subpopulation of individuals initially put in for a clearance.) The expectation, then, is that individuals granted clearance on appeal have relatively comparable demographics to those who were granted clearances without an appeal. The question, then, is if appellants with unsuccessful appeals are comparable to the non-cleared civilian security workforce or the general civilian population. These relationships of populations are visualized in Figure 5 below.

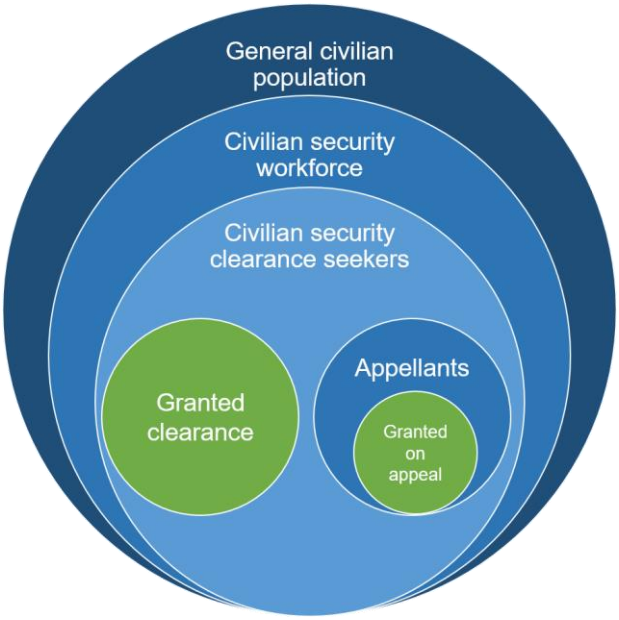

Figure 5: Population Relationships

With established baselines for individuals that have been granted clearances, investigators may be able to prioritize a) resources for more high-risk applicants for more intensive investigations or b) resolving low-risk applicants given what is initially gleaned from the SF-86.

6.1.2 Privacy Concerns and Intelligence Gathering by Adversaries

Another longer-term opportunity may include analysis of the likelihood and techniques possible for re-identification of individuals within the data set. Given the sensitivity of some of the information disclosed within the SF-86, and by extension throughout the appeals process, a public repository of such data should consider the risk of re-identification. Aside from the obvious privacy implications, once re-identified, individuals may be subject to compromise or coercion attempts by adversaries. After all, if an individual had a successful appeal and they could be identified, then an adversary could have an idea of which cleared individuals may be vulnerable to exploitation. Furthermore, adversaries could target appellants with former military or cleared work experience in particular given the impact of the Office of Personnel Management (OPM) breach (Nakashima, 2015).

6.2 Replication with Similar Datasets

The identification of additional data sources outside of the DOHA set pertaining to security decisions could serve to increase understanding of preferences and standards related to clearance beyond the Department of Defense. The Department of Energy hosts a similar repository of cases online (Department of Energy, 2018). For next steps, scraping and downloading the Department of Energy's public security case archive to test the reproducibility of these methods and results is advisable.

6.3 Outreach to the Defense Industry

The overall goal of this work was to provide insight on decision-making for the defense industry's benefit. Evaluation of hiring processes within the industry to measure fit with the adjudicative guidelines and the results obtained may uncover institutional knowledge regarding the clearance process. Likewise, surveys and assessments of the breadth and robustness of Employee Assistance Programs (EAPs) relative to adjudicative guidelines with individual employers may assist in their efforts to help their employees maintain their clearances.

National economic crises (related to 9/11, Hurricane Katrina, and the housing / mortgage crisis) affected many working in the defense industry, a la the "traumatic life events" feature. Moving forward, employers and investigators should remember that not every eventuality can be prepared for, so employees may raise "red flags" due to no fault of their own. Likewise, applicants should do their best to contextualize how nationwide issues have impacted their present circumstances if that is the case for them.

6.3.1 Dataset Indexing

With some initial effort, given how easily the dataset was scraped, it would be possible to develop a web interface or index for easy review of the clearance appeals. Industrial security practitioners could use that search utility for training efforts with the workforces that they serve. For instance, if an applicant had a concern about a particular issue in their past, they could see the potentially negative outcome of falsifying that issue, or the positive outcomes associated with taking steps to address it. Alternatively, the specific cases could be used as case studies if nothing else.

6.4 Proposed 4-C Model

In response to the case outcomes and judgment summaries, a simple mnemonic called the "4-C Model" was developed to summarize the variety of mitigating factors associated with the 13 adjudicative guidelines, which is detailed below.

6.4.1 Candor

- Do not omit information from your SF-86 application because you think it could be damaging.
- Answer questions honestly during interviews with facility security officers, DSS, or OPM investigators.
- Be open and willing to respond to challenging questions during any DOHA hearings.

6.4.2 Compliance

- Comply with the rule of law before and after submitting a clearance application.
- Comply with the standards and expectations of the clearance process.
- Comply with your employers' respective security policies.
- Use common sense and due diligence when handling classified information.

6.4.3 Commitment

- Demonstrate a commitment to family, particularly to those that are U.S. citizens.

- Demonstrate commitment to a community of practice, or a physical community in which you live through volunteering, etc.
- Demonstrate a commitment to your employer by making yourself at asset at work and providing two weeks' notice should you choose to leave.
- Demonstrate a commitment to keeping finances and assets within the U.S. by forgoing foreign bank accounts, stocks, and property ownership.

6.4.4 Contributions

- Contribute to U.S. national security by keeping classified information safe.
- Provide evidence of preference of the U.S. over other nations, perhaps by forgoing dual-citizenship.
- Demonstrate a willingness to put one's self in harm's way for the sake of others by serving in or with the U.S. military.

Moving forward, as part of efforts to work with the defense industry, a next step would be to provide this model to facility security officers and test its applicability and usability as a guideline for completing security clearance applications. Additionally, using such a model may be complementary to raising awareness of insider threats within the defense industry and federal government.

7 Bibliography

Burkett, R. (2013, March). An Alternative Framework for Agent Recruitment: From MICE to RASCLS. *Studies in Intelligence, 57*(1), 7-17.

Casey, T. (2015). *A Field Guide to Insider Threat.* Retrieved from Intel: http://www.intel.com/content/dam/www/public/us/en/documents/best-practices/a-field-guide-to-insider-threat-paper.pdf.

Coats, D. R. (2017). *Statement for the Record Worldwide Threat Assessment of the US Intelligence Community.* Office of the Director of National Intelligence. Retrieved from https://www.dni.gov/files/documents/Newsroom/Testimonies/SSCI%20Unclassified%20SFR%20-%20Final.pdf

Costa, D. (2017, March 7). *CERT Definition of 'Insider Threat' - Updated.* Retrieved from SEI Insights: Insider Threat Blog: https://insights.sei.cmu.edu/insider-threat/2017/03/cert-definition-of-insider-threat---updated.html

Costa, D., Albrethsen, M., Collins, M., Pel, S., Silowash, G., & Spooner, D. (2016). *An Insider Theat Indicator Ontology (CMU/SEI-2016-TR-007).* Pittsburgh: Software Engineering Institute, Carnegie Mellon University. Retrieved from http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=454613

Defense Office of Hearing and Appeals. (2018). *Industrial Security Clearance Decisions*. Retrieved from ogc.osd.mil/doha/industrial/

Department of Energy. (2018). *Security Cases*. Retrieved May 10, 2017, from https://energy.gov/oha/security-cases

Fung, B. (2014, March 23). 5.1 Million Americans have security clearances. That's more than the entire population of Norway. *The Washington Post*. Retrieved from https://www.washingtonpost.com/news/the-switch/wp/2014/03/24/5-1-million-americans-have-security-clearances-thats-more-than-the-entire-population-of-norway/?utm_term=.3bd2242144b3

Gibson, C. (2014). For domestic violence victims, abusers' security clearances add an extra layer of fear. *The Washington Post*. Retrieved May 1, 2017, from https://www.washingtonpost.com/local/for-domestic-violence-victims-abusers-security-clearances-add-an-extra-layer-of-fear/2014/05/17/b281e63a-ca64-11e3-93eb-6c0037dde2ad_story.html?utm_term=.556eed71dd88

Lawrence, Q. (2016). *After Combat Stress, Violence Can Show Up At Home.* Retrieved from NPR: http://www.npr.org/sections/health-shots/2016/04/27/475908537/after-combat-stress-violence-can-show-up-at-home

McGarvey, D. (2017, April). Want to Plug Intel Leaks? Let Technology Find the Next Insider Threat. *Defense One*. Retrieved from http://www.defenseone.com/ideas/2017/04/want-plug-intelligence-leaks-let-modern-technology-background-checks/136729/

Nakashima, E. (2015, July 9). Hacks of OPM databases compromised 22.1 million people, federal authorities say. *The Washington Post*. Retrieved November 9, 2018, from The Washington Post: https://www.washingtonpost.com/news/federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say/?noredirect=on&utm_term=.0ccf71576bc6

Shaw, E., & Sellers, L. (2015, June). Application of the Critical-Path Method to Evaluate Insider RIsks. *Studies in Intelligence, 58*(2), 1-8.

Stein, J. (1994). The Mole's Manual. *The New York Times, 5*, p. 16. Retrieved April 30, 2017, from http://www.nytimes.com/1994/07/05/opinion/the-mole-s-manual.html

U.S. Bureau of Labor Statistics. (2016). *Census of Fatal Occupational Injuries, 2016.* Retrieved from Census of Fatal Occupational Injuries (CFOI) - Current and Revised Data : https://www.bls.gov/iif/oshwc/cfoi/cfch0015.pdf

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
(Leave Blank)	Month and Year (date added at time of publication)	Final

4. TITLE AND SUBTITLE	5. FUNDING NUMBERS
Data Analysis of Security Clearance Appeal Decisions	FA8702-15-D-0002

6. AUTHOR(S)

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213	CMU/SEI-2018-SR-XXX

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSORING/MONITORING AGENCY REPORT NUMBER
AFLCMC/PZE/Hanscom Enterprise Acquisition Division 20 Schilling Circle Building 1305 Hanscom AFB, MA 01731-2116	n/a

11. SUPPLEMENTARY NOTES

12A DISTRIBUTION/AVAILABILITY STATEMENT	12B DISTRIBUTION CODE
Unclassified/Unlimited, DTIC, NTIS	

13. ABSTRACT (MAXIMUM 200 WORDS)

14. SUBJECT TERMS	15. NUMBER OF PAGES
insider threat; espionage; Department of Defense (DoD); security clearances; appeal decisions; decision-making; correlations; binary logistic regression	34

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UL

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89) Prescribed by ANSI Std. Z39-18
298-102