PERSEREC

OPA-2019-021
PERSEREC-TR-19-02

March 2019

The Resource Exfiltration Project: Findings from DoD Cases, 1985-2017

Stephanie L. Jaros
Defense Personnel and Security Research Center
Office of People Analytics

Katlin J. Rhyner
Shannen M. McGrath
Erik R. Gregory
Northrop Grumman Technology Services

OPA
OFFICE OF PEOPLE ANALYTICS

Approved for Public Distribution
Defense Personnel and Security Research Center
Office of People Analytics

OPA-2019-021 **PERSEREC-TR-19-01** **March 2019**

The Resource Exfiltration Project: Findings from DoD Cases, 1985-2017

Stephanie L. Jaros
Defense Personnel and Security Research Center, Office of People Analytics

Katlin J. Rhyner, Shannen M. McGrath, Erik R. Gregory
Northrop Grumman Technology Services

Released by – Eric L. Lang

Defense Personnel and Security Research Center
Office of People Analytics
400 Gigling Road, Seaside, CA 93955

REPORT DOCUMENTATION PAGE	**Form Approved** **OMB No. 0704-0188**

The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE: March 2019	2. REPORT TYPE: Technical Report	3. DATES COVERED:

4. TITLE: The Resource Exfiltration Project: Findings from DoD Cases, 1985-2017	5a. CONTRACT NUMBER:
	5b. GRANT NUMBER:
	5c. PROGRAM ELEMENT NUMBER:
6. AUTHOR(S): Stephanie L. Jaros, Katlin J. Rhyner, Shannen M. McGrath, Erik R. Gregory	5d. PROJECT NUMBER:
	5e. TASK NUMBER:
	5f. WORK UNIT NUMBER:
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES): Defense Personnel and Security Research Center Office of People Analytics 400 Gigling Road Seaside, CA 93955	8. PERFORMING ORGANIZATION REPORT NUMBER PERSEREC: There are two report numbers: PERSEREC-TR-19-02 OPA-2019-021
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES):	10. SPONSORING/MONITOR'S ACRONYM(S):
	11. SPONSORING/MONITOR'S REPORT NUMBER(S):

12. DISTRIBUTION/AVAILABILITY STATEMENT: A

13. SUPPLEMENTARY NOTES:

ABSTRACT: In recognition of the persistent and evolving insider threat to the integrity of DoD resources, the Defense Personnel and Security Research Center expanded its flagship research project on espionage to include all publicly known cases of resource exfiltration, or cases that involved the intentional and unauthorized removal of DoD resources from authorized locations regardless of classification level. The objective of this study was to identify common themes and behavioral indicators that preceded individuals' arrests in order to prevent and mitigate future incidents. In total, 83 cases of DoD resource exfiltration were included in this study, and researchers collected information related to 392 variables of interest, to include pre-arrest behavior that matched disqualifying factors of the Adjudicative Guidelines and/or behavioral threat assessment themes. Researchers concluded that there is no demographic profile of individuals who exfiltrate DoD resources, but there are common behavioral indicators that represent intervention points, or those points in a person's transformation from a trusted employee to an insider threat when DoD could take action to hopefully bring that person back into the productive workforce.

14. SUBJECT TERMS: resource exfiltration, insider threat, espionage, unauthorized disclosure, leaks, mitigation

15. SECURITY CLASSIFICATION OF: Unclassified			16. LIMITATION OF ABSTRACT:	17. NUMBER OF PAGES: 35	19a. NAME OF RESPONSIBLE PERSON: Eric L. Lang, Director
a. REPORT: Unclassified	b. ABSTRACT: Unclassified	c. THIS PAGE:			19b. TELEPHONE NUMBER (Include area code): 831-583-2846

Standard Form 298 (Rev. 8/98)
Prescribed by ANSI td. Z39.18

PREFACE

In the aftermath of the John Walker spy scandal, DoD established the Defense Personnel and Security Research Center (PERSEREC). Since its founding, PERSEREC has been committed to helping DoD stakeholders better detect, prevent, and mitigate malicious insider threats, to include espionage and unauthorized disclosures. This report is the latest contribution to that effort, and is designed to provide DoD stakeholders with empirically based, operationally relevant behavioral indicators that signal potential future threats and opportunities for intervention.

Eric L. Lang
Director, PERSEREC

ACKNOWLEDGEMENTS

The authors would like to thank Peter Chetirkin, Julie Fenderson, Bradley Latendresse, Sarah Limyansky, and Ryan Van Vechten for their research assistance.

EXECUTIVE SUMMARY

INTRODUCTION

Despite changes in policies and practices over the years, perpetrators continue to exfiltrate resources from DoD and transmit them to unauthorized recipients. In recognition of this persistent and evolving insider threat, the Defense Personnel and Security Research Center (PERSEREC) examined cases of resource exfiltration, or cases that involve the intentional and unauthorized removal of DoD resources from authorized locations, to identify potential intervention points along perpetrators' pathways to criminal behavior. The purpose of this project was to analyze the current state of resource exfiltration and provide operationally relevant, empirically based recommendations to DoD stakeholders in order to improve efforts to detect, prevent, and mitigate these insider threats.

METHOD

Eligible cases included those perpetrators who: 1) had exfiltrated a DoD resource; 2) had been arrested after November 19, 1985, the publication date of the report issued by the *Commission to Review DoD Security Policy and Practices*; and 3) had been convicted or pled guilty by December 31, 2017. These criteria resulted in 83 eligible perpetrators.

All information gathered for this project was publicly available. A codebook containing 392 variables organized into eight categories was created for this project. These eight categories were designed to capture the perpetrators' characteristics, the circumstances surrounding the incident, and pre-arrest behavioral indicators that signaled malicious intent and therefore, intervention opportunities, along the pathway to exfiltration.

RESULTS

Nearly all of the perpetrators were male. They varied by age, citizenship, marital status, parental status, and education. Most exfiltration careers lasted less than 2 years, and nearly all ended within 10 years. To remove resources, perpetrators most often carried them out the door of a secure facility, usually concealed in an everyday object such as a bag or briefcase. Among those who transmitted material to a foreign entity, Russia was the most common recipient. The most common motive was money, followed by ideology.

Researchers broke down the 13 Adjudicative Guidelines into 75 disqualifying factors in order to identify pre-arrest behavioral indicators. The 10 most common disqualifying factors clustered in four of the 13 Adjudicative Guidelines (i.e., Guideline B: Foreign Influence, Guideline C: Foreign Preference, Guideline E: Personal Conduct, and Guideline K: Handling Protected Information). In contrast, the least common disqualifying factors clustered in Guideline D: Sexual Behavior, Guideline F: Financial

Considerations, Guideline G: Alcohol Consumption, Guideline H: Drug Involvement, and Guideline L: Outside Activities.

Researchers also leveraged the behavioral threat assessment framework (Fein & Vossekuil, 1997) in order to identify potential indicators. Overall, 65 out of the 83 perpetrators (78%) exhibited behavior that corresponded with at least one of the 10 behavioral threat assessment variables. Notably, nearly one-quarter of all perpetrators talked about their exfiltration activities to someone who was neither a handler nor an accomplice, and in 32 out of the 83 cases, people noticed concerning behavior or changes in behavior prior to the perpetrators' arrests.

FINDINGS & RECOMMENDATIONS

Finding #1: User activity monitoring enables DoD to observe the electronic movement of its resources, but there appears to be insufficient protections against unauthorized physical movement.

> **Recommendation #1:** Where possible, DoD should reduce the number of locations within a facility where critical electronic assets can be printed and/or physically reproduced. Then, DoD should institute random physical inspections, again when possible.

Finding #2: The majority of perpetrators exhibited pre-arrest behavioral indicators, but the behavioral threat assessment framework appears to yield more actionable results than those indicators derived from the disqualifying factors associated with the Adjudicative Guidelines.

> **Recommendation #2:** DoD should integrate best practices for behavioral threat assessment into the insider threat training mandated by the *National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs* for both Insider Threat Program Personnel (Section F) and the general workforce (Section I).

Finding #3: Employees who experience professional stressors, such as a demotion, could target DoD for retaliation against perceived wrongs.

> **Recommendation #3:** DoD should ensure that its personnel who issue disciplinary notices are trained in conflict resolution and/or de-escalation strategies, and security personnel should be on hand to ensure those who are terminated do not retain physical or logical access. DoD also should prioritize additional research to identify best practices to reintegrate employees into the workforce after serious disciplinary action, such as a demotion or suspension. Together with wellness programs such as Employee Assistance Programs, these practices should help to ensure employees successfully recover from difficult events and situations.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

INTRODUCTION

In the aftermath of the John Walker spy ring, then-Secretary of Defense Caspar Weinberger established the *Commission to Review DoD Security Policy and Practices*. Members of this commission, known informally as the Stilwell Commission, recognized that DoD could never eliminate the loss of classified secrets, but steps could be taken to make espionage, theft, and other unauthorized disclosures more difficult.

In addition to establishing the Defense Personnel and Security Research Center (PERSEREC), the Stilwell Commission recommended the following: "Establish a policy that all briefcases and similar personal belongings are subject to search upon entry and exit from DoD installations to determine if classified information is being removed without authority" (p.9). Presumably, for reasons of impracticality—for example, more than 25,000 people pass in and out of just the Pentagon every day—DoD did not adopt this recommendation.

Malicious insider threat behavior persists, and cases continue to surpass one another in the threat they pose to national security. For example, in October 2001, authorities arrested Brian Regan in what was then "the biggest heist of classified information in the history of American espionage" (Bhattacharjee, 2016). Altogether, Regan stole more than 20,000 pages of documents, which he carried out in his gym bag. More recently, in August 2016, authorities arrested Harold Martin III, a government contractor who stands accused of what is *now* "thought to be the largest theft of classified government material ever" (Nakashima, 2016). Enabled by time and technology, Martin allegedly stole 50 terabytes of data from his government client over two decades, in both hard copy and digital form, which he stored in his home, his car, and his shed. In an article about Martin, one former employee explained, "Disneyland has more physical security checks than we had" (Nakashima & Zapotosky, 2016, p. 4).

People rarely join organizations with an intent to do harm (Smith, Jaros, & Chandler, 2016). Instead, they transform over time from trusted employees into malicious insider threats. During that time, DoD has a window of opportunity to detect and respond to any behavioral indicators that often precede these high-impact, low-frequency events (MITRE Corporation, 2009). These behavioral indicators represent potential intervention points, or opportunities for DoD commanders and civilian leaders to disrupt the pathway to resource exfiltration and bring employees back into the productive workforce.

CURRENT STUDY

In recognition of the persistent and evolving insider threat to the integrity of DoD resources, PERSEREC has expanded its flagship research project on espionage to include all known cases of resource exfiltration, or cases that involve the intentional and unauthorized removal of DoD resources from authorized locations regardless of future transmission. The purpose of this project is to analyze the current state of resource exfiltration and provide operationally relevant, empirically based recommendations to DoD stakeholders in order to improve efforts to detect, prevent, and mitigate these insider threats. The goals of this project are as follows:

- Analyze trends across resource exfiltration cases;
- Identify common behavioral indicators that preceded arrests; and
- Recommend steps to secure DoD resources based on identified trends.

METHOD

All of the material collected for this project was publicly available (hereinafter, "open source intelligence.") What follows is an overview of the research design, from case selection through data collection and analysis.

ELIGIBILITY CRITERIA

Cases were selected for inclusion based on three eligibility criteria. First, perpetrators had to exfiltrate a resource, whether physical or digital, that DoD created or owned wholly or in-part. Because of this criterion, all but one of the perpetrators were current or former DoD civilian employees, Service members, or contracting personnel. Second, in order to maximize the relevance of the cases and ensure that all data could be analyzed within the project timeline, perpetrators had to have been arrested after the Stilwell Commission Report was issued on November 19, 1985. This date was selected because it marked a point in time when DoD publicly focused its attention on efforts to minimize insider threats to its resources. Third, perpetrators must have been convicted of or pled guilty to an exfiltration-related crime by December 31, 2017. In total, 83 cases of DoD resource exfiltration met these criteria and were included in this study.

DATA ORGANIZATION

A codebook containing 392 variables of interest organized into eight categories was created for this project. These eight categories were structured to capture the characteristics of the perpetrator, the circumstances surrounding the exfiltration event, perpetrators' motive(s), and pre-arrest behavioral indicators.

The *Demographic* and *Employment* categories included variables related to the perpetrator's background and demographic characteristics at both the time exfiltration began and at the time of arrest, such as employment, age, parental status, and education. The *Initiation* category included variables related to how each perpetrator became involved in exfiltration, whether as a recruit, volunteer, and/or subject of a "sting" operation. In addition, this category included variables specific to those perpetrators who exfiltrated DoD resources without any apparent attempt to transmit. These perpetrators were coded separately to allow for any potential differences between their motives, methods, and characteristics and those of people who transmitted resources. The *Exfiltration* category included variables related to the exfiltration event itself, including, but not limited to, how resources were removed from an authorized location and, if relevant, the identity of the intended unauthorized recipient. Variables related to *Judicial Outcome* also were collected, such as date of arrest and judicial outcome, as were variables related to *Motive*.

In an effort to identify intervention points prior to exfiltration, each perpetrator's pre-arrest behavior was assessed to determine whether it matched any of the 75 disqualifying factors associated with the 13 *Adjudicative Guidelines for Determining Eligibility for Access to Classified Information* (2005) (hereinafter, "Adjudicative

Guidelines”). (See Appendix A for the list of Adjudicative Guidelines broken down into their disqualifying factors.)

Finally, behavioral threat assessment has become “the standard of care for preventing violence in schools, colleges, and the workplace and against government and other public officials” (APA, 2013: p. 2), and has been applied to studies of non-violent criminal behavior (e.g., Shaw & Fischer, 2005). Variables were derived from five *Behavioral Threat Assessment* themes: Concerning Communications, Concerning Interests, Planning Behavior, Significant Life Events, and Concerned Others (Borum, Fein, Vossekuil, & Berglund, 1999).

DATA COLLECTION AND ANALYSIS

Open source intelligence for each case was independently reviewed and coded by two trained behavioral research scientists. Upon completion of their independent efforts, the results were reviewed and compared. Discrepancies were resolved by re-analyzing open source intelligence. If the two researchers could not reach concurrence on a variable or set of variables, open source intelligence was reviewed and the discrepancy was resolved by a third trained behavioral research scientist. After finalizing a case, the results were entered into the Resource Exfiltration Statistical Package for the Social Sciences (SPSS) Database for descriptive analyses.

RESULTS

Researchers organized their descriptive analyses in accordance with six key questions intended to summarize perpetrators' resource exfiltration activities: who, what, when, how, where, and why. Then, they turned their attention to potential intervention points as highlighted by an analysis of the pre-arrest behavioral indicators associated with the Adjudicative Guidelines and behavioral threat assessment themes. As is the case with most research that relies on open source intelligence, information was inconsistent or missing for many variables. Researchers designated missing information as "Unknown" in the overview of the results that follow.

THE WHO: OVERVIEW OF THE PERPETRATORS

Table 1 displays six demographic variables for the 83 perpetrators based on the date that resource exfiltration began. (See Appendix B for a description of how researchers constructed this date.) While conclusive information was not available in open source intelligence for a number of perpetrators, a summary of known demographic results is as follows.

Nearly all of the perpetrators were male (n=79). They ranged in age from 15 to 66, with a mean and median age of 35. More than one-third were between 20 and 29 when they began their resource exfiltration careers (n=29). Of the 57 perpetrators for whom open source information was available, 40 were native-born U.S. citizens and 17 were foreign born, naturalized citizens. Twenty-nine perpetrators were married when resource exfiltration began and 58 did not have children. Of the 44 perpetrators for whom open source intelligence included education information, 16 had a high school degree or its equivalent, and 21 had a college degree or higher.

Table 1
Perpetrator Demographics When Exfiltration Began (N=83)

Demographic Category when Exfiltration Began	Count
Age Group	
<20	3
20-29	29
30-39	22
40-49	17
50-59	9
60-69	2
Unknown	1
Gender	
Male	79
Female	4
Citizenship	
Native Born	40
Foreign Born/Naturalized	17
Unknown	26
Marital Status	
Never Married	8
Married	29
Divorced	4
Widowed	0
Unknown	42
Parental Status*	
Children	25
No Children	58
Education	
Doctorate	7
Professional Degree	1
Masters	4
Bachelor’s	9
Some College, No Degree	6
High School Graduate (or Equivalent)	16
High School, No Diploma	1
Unknown	39

*If open source intelligence provided no indication of children when exfiltration began, researchers coded the case as “No Children”.

As Table 2 indicates, over half of the perpetrators were Service members when they began their exfiltration careers (n=44). Of these 44 perpetrators in the military, nearly half were in the Army (n=20), which corresponds with the Army’s size relative to the other Service branches.

Table 2
Perpetrator Occupation When Exfiltration Began (N=85)*

Occupation when Exfiltration Began	Count
Military	
Air Force	5
Army	20
Coast Guard	0
Marine Corps	4
Navy	15
Not In the Labor Force (e.g., retired)	3
Private Sector, Not a Government Contractor	3
Private Sector, Federal Government Contractor	12
Federal Government Employee	18
State or Local Government Employee	1
Unemployed	0
Unknown	4

*Table total exceeds 83 because two individuals held concurrent employment both in the military and in a non-military occupation at the time resource exfiltration began.

Open source intelligence included clearance information for 70 of the 83 perpetrators. As shown in Table 3, among those for whom information was available, most perpetrators held a Top Secret (TS) clearance (n=14) or a TS clearance with access to Sensitive Compartmented Information (TS/SCI) (n=14) at the time exfiltration began.

Clearance levels often change throughout an individual's career, and so, when possible, researchers noted the highest clearance ever held by each perpetrator, which includes both before and after the onset of exfiltration. As summarized in Table 3, 21 perpetrators attained a TS clearance at some point during their careers, while an additional 19 held TS/SCI.

Table 3
Perpetrator Clearance Level When Exfiltration Began (N=83)

Clearance Level at Time Exfiltration Activities Began	Count
TS/SCI	14
TS	14
Secret	12
Confidential	0
Held Clearance, Level Unknown	13
No Clearance	17
Unknown	13
Highest Known Clearance Ever Held	**Count**
TS/SCI	19
TS	21
Secret	18
Never Held a Clearance	7
Unknown	18

THE WHAT: OVERVIEW OF THE RESOURCES

Open source intelligence rarely included the precise classification of every resource that perpetrators exfiltrated. To get a general sense of the risk to classified versus unclassified resources, researchers captured the highest classification of the resources noted for each perpetrator. Open source intelligence did not include relevant information for 27 perpetrators (i.e., Unknown), and only noted that the resources were classified for an additional 21 perpetrators (i.e., the specific classification level was not included). Among the remaining 35 perpetrators, 16 exfiltrated resources up to the Secret level and 10 exfiltrated resources up to the TS level, as shown in Table 4.

Table 4
Highest Classification Level of Exfiltrated Material (N=83)

Clearance Level	Count
SCI	3
TS	10
Secret	16
Unclassified	6
Classified, Specific Level Unknown	21
Unknown	27

When possible, researchers paired the perpetrators' highest known clearance level with the highest classification of the resources they exfiltrated. Open source intelligence included this information for 23 perpetrators, none of whom exfiltrated resources that were classified above their own clearance levels. In other words, no one with a Secret clearance exfiltrated TS resources. Over the course of their careers, many perpetrators exfiltrated resources classified at lower levels than their own highest clearances, but the data do not allow for a more specific analysis.

THE WHEN: OVERVIEW OF THE TIMELINE

For nearly all of the cases (n=79), researchers were able to calculate the length of each perpetrator's exfiltration career based on the date exfiltration began and the date of arrest. Figure 1 shows a significant decline after two years of exfiltration activity. Thirty-two perpetrators were active for two years or less, and 68 were active for 10 or fewer years. Notably, of the four women included in this study, two were among the 11 who had exfiltration careers that lasted longer than 10 years: Ana Montes and Theresa Squillacote.

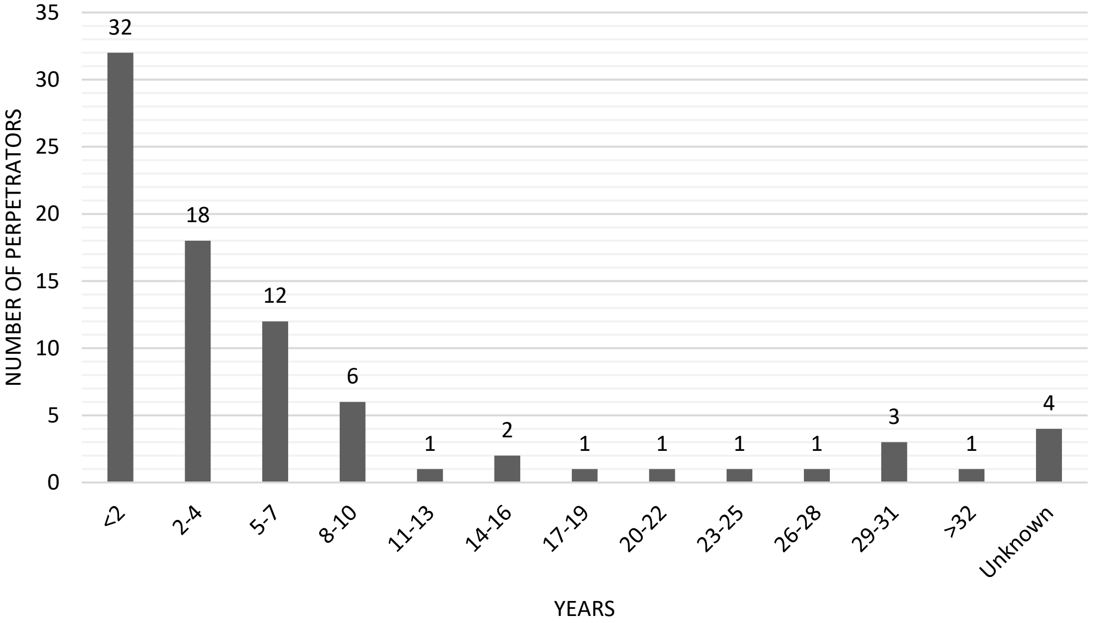

Figure 1 Length of Exfiltration Careers (N=83)

THE HOW: OVERVIEW OF EXFILTRATION

In addition to coding the who, the what, and the when, researchers coded how perpetrators moved in and out of their exfiltration careers followed by how they exfiltrated resources. First, researchers coded perpetrators as volunteers, recruits, and/or subjects of "sting" operations over their exfiltration careers. Volunteers were those who approached and made an offer to an unauthorized recipient (n=47), while recruits were those approached by unauthorized recipients (n=24). Researchers coded anyone who was at some point in contact with an undercover law enforcement agent or asset as the subject of a sting operation (n=28). Seven perpetrators did not fall into any of these categories because, even though they exfiltrated resources, there was no record that they attempted to transmit anything and, therefore, no record that they interacted with an unauthorized recipient.

Second, open source intelligence included information relevant to how 45 perpetrators exfiltrated DoD resources. Of these 45, 17 perpetrators exited an authorized location with the resources concealed in a container of some kind, usually a briefcase or gym bag. Seven perpetrators exited with the resources concealed on their persons (e.g., under a hat or jacket, in pants). Ten perpetrators exfiltrated resources from an authorized location via email or fax, and four misused their courier cards. Notably, 10 perpetrators never physically exfiltrated anything. Instead, they intentionally memorized information for later transmission.

THE WHERE: OVERVIEW OF RECIPIENTS

Nearly all of the perpetrators included in this study attempted to transmit or successfully transmitted resources to an unauthorized recipient (n=76). Open source intelligence included specific information about the actual or intended recipients for 71 of these 76 cases. The majority (n=63) of the perpetrators exfiltrated resources to a foreign entity, whether it was a person, organization, or government. Perpetrators exfiltrated on behalf of Russia (n=25), followed by China (n=13), East Germany (n=5), and Israel (n=4). Less common foreign recipients included Iran, Cuba, and Al Qaeda. Three perpetrators exfiltrated resources to journalists, and two gave information to other U.S. citizens (i.e., a non-DoD anti-terrorism unit leader and a lawyer). One perpetrator attempted to pass information to multiple entities, and one gave resources to an archive.

THE WHY: OVERVIEW OF MOTIVE

Open source intelligence referenced at least one motive for 79 of the 83 perpetrators. Forty of the 79 perpetrators had only one motive noted. On average, perpetrators had two motives.

As shown in Table 5, money proved to be the most common motive (n=40). This includes perpetrators who needed money because of financial challenges, and those motivated by greed. Ideology, or the desire to further a belief or commitment to an issue or cause (e.g., opposition to a U.S. Government policy or action), motivated 25 perpetrators. For example, Thomas Drake leaked classified information in response to his opposition to domestic spying practices. In contrast, divided loyalties motivated nine perpetrators, such as Dongfan (Greg) Chung who was proud of how much money he had saved Boeing and his work for the U.S., but also wanted to help China. After his arrest, he said he never wanted to hurt the U.S.; he only wanted to help China. Among the motives coded as “Other”, one perpetrator received gift cards and baseball tickets, while another wanted the Soviet Union to send him to college.

Open source intelligence noted changes in motive over time for four perpetrators. For example, one perpetrator initially sought revenge, but once that need was satisfied, he continued to exfiltrate resources for monetary gain.

Table 5
All Known Motives*

Motive Category	Count
Money	40
Ideology: Intended to further an ideological belief or commitment to an issue, including opposition to a U.S. Government policy or action	25
Revenge: Desire to get even or get back at a person, group, or organization	13
Career: Desire to improve future career opportunities	13
Excitement: Desire for thrills and/or fame	11
Divided Loyalty: Divided allegiance between two countries	9
Ingratiation: Desire to influence, manipulate, or control a person, group, or organization by becoming more attractive or likeable	9
Blackmail: Real or perceived threat of coercion	5
Honeytrap: Desire to please an intimate partner who was later confirmed to be or assumed to be a honeytrap	2
Other	19

* Total exceeds 83 because perpetrators could have multiple motives.

BEHAVIORAL INDICATORS

In order to identify potential intervention points prior to exfiltration, researchers coded perpetrators' pre-arrest behaviors in accordance with two sets of potential indicators. First, they coded behaviors in accordance with the disqualifying factors for the 13 Adjudicative Guidelines. Second, they coded behaviors associated with behavioral threat assessment themes. What follows is an overview of the results.

Disqualifying Factors for the Adjudicative Guidelines

Overall, perpetrators demonstrated pre-arrest behavior that corresponded with at least one disqualifying factor associated with all 13 Adjudicative Guidelines prior to their arrest. In fact, as shown in Figure 2, all 83 perpetrators (100%) engaged in some kind of behavior that corresponded with at least one of the disqualifying factors included in Guideline K: Handling Protected Information, with Guideline E: Personal Conduct close behind (n=82).

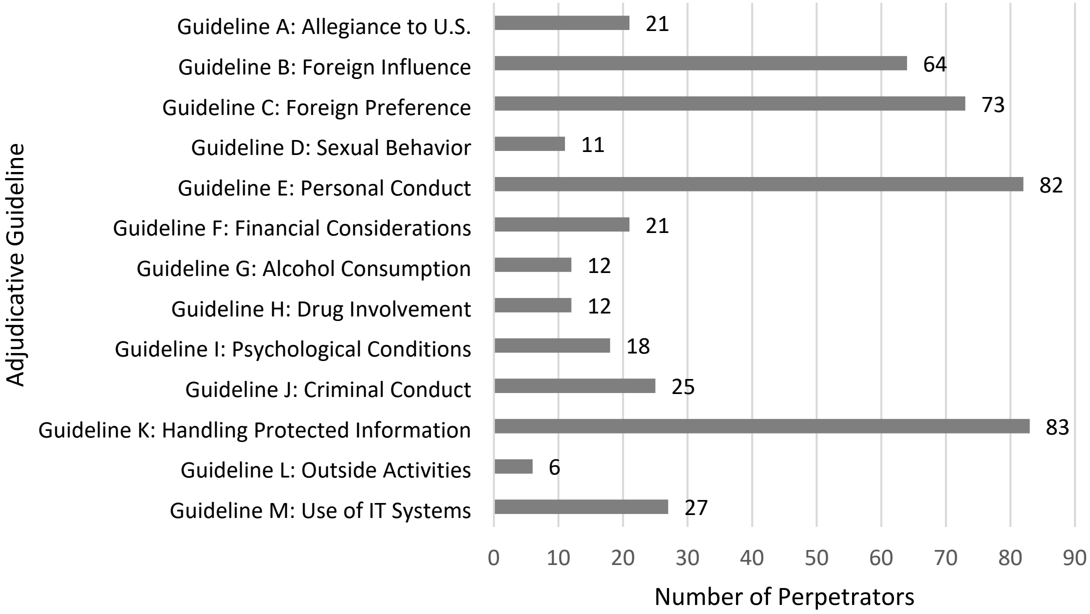

Figure 2 Perpetrator Pre-Arrest Behavior Categorized by Adjudicative Guideline (N=83)

In an effort to understand perpetrators' specific behavioral indicators, researchers broke down Figure 2 into the 75 disqualifying factors that comprise the 13 Adjudicative Guidelines. While the results for all 75 factors are available in Appendix A, Table 6 lists the 10 disqualifying factors, broken down by Adjudicative Guideline, which most often matched behavior exhibited by perpetrators prior to their arrests.

Table 6
Ten Disqualifying Factors that Most Often Matched Perpetrator Pre-Arrest Behavior

ADJUDICATIVE GUIDELINE & DISQUALIFYING FACTOR	COUNT
GUIDELINE B: FOREIGN INFLUENCE	
Person had contact with a foreign family member, business or professional associate, friend, or other person who was a citizen of or resident in a foreign country, which could have created a heightened risk of foreign exploitation, inducement, manipulation, pressure, or coercion. *Include all countries regardless of relationship with the United States. Do not include a person's handler or anyone posing as a handler.**	44
Person had connections to a foreign person, group, or government that could have created a potential conflict of interest between the individual's obligation to protect sensitive information or technology and the individual's desire to help a foreign person, group, or country by providing that information. *Include all countries regardless of relationship with the United States. Do not include a person's handler or anyone posing as a handler.*	40
Person failed to report, when required, association with a foreign national, *to include a person's handler or anyone posing as a handler. Include all countries regardless of relationship with the United States.*	42
GUIDELINE C: FOREIGN PREFERENCE	
Person performed or attempted to perform duties, or otherwise acted, so as to serve the interests of a foreign person, group, organization, or government in conflict with the National security interest.	71
GUIDELINE E: PERSONAL CONDUCT	
Person engaged in untrustworthy or unreliable behavior to include breach of client confidentiality, release of proprietary information, unauthorized release of sensitive corporate or other government-protected information.	79
Person misused government or other employer's time or resources *(i.e., personnel, facilities, accesses, equipment).*	65
Person violated a written or recorded commitment made by the individual to the employer as a condition of employment.	80
GUIDELINE K: HANDLING PROTECTED INFORMATION	
Person engaged in deliberate or negligent disclosure of classified or other protected information to unauthorized persons, including, but not limited to, personal or business contacts, to the media, or to persons present at seminars, meetings, or conferences.	74
Person collected or stored classified or other protected information at home or in any other unauthorized location.	65
Person failed to comply with rules for the protection of classified or other protected information.	81

* Italicized text added to the disqualifying factor for clarification purposes for this project.

As shown in Table 6, the 10 most common disqualifying factors clustered in four of the 13 Adjudicative Guidelines (i.e., Guideline B: Foreign Influence, Guideline C: Foreign Preference, Guideline E: Personal Conduct, and Guideline K: Handling Protected Information). In contrast, the least common disqualifying factors clustered in Guideline

D: Sexual Behavior, Guideline F: Financial Considerations, Guideline G: Alcohol Consumption, Guideline H: Drug Involvement, and Guideline L: Outside Activities (See Appendix A).

Behavioral Threat Assessment

In addition to the disqualifying factors associated with the 13 Adjudicative Guidelines, researchers reviewed open source intelligence for behaviors associated with five themes found in the behavioral threat assessment literature: Concerning Communications, Concerning Interests, Planning Behavior, Significant Life Events, and Concerned Others. Like the Adjudicative Guidelines, perpetrators' pre-arrest behaviors could fall into multiple behavioral threat assessment themes, and each behavioral threat assessment theme was broken down into a number of variables. Table 7 presents the full results of the behavioral threat assessment analysis.

Table 7
Perpetrator Pre-Arrest Behavior Organized by Behavioral Threat Assessment Theme

THREAT ASSESSMENT THEME & VARIABLE	Count
Concerning Communications	
Prior to arrest, perpetrator spoke about exfiltration activity to at least one other person who was not an accomplice, a handler, or someone posing as a handler	21
Concerning Interests	
Prior to arrest, perpetrator showed concerning interests related to exfiltration (e.g., interested in surveillance technology, attended anti-government protests)	12
Planning Behavior	
Perpetrator sought out a specific career/job with the intent to exfiltrate resources (e.g., refused promotions to maintain access to classified information)	9
Perpetrator planned exfiltration (e.g., scoped dead drops, developed cover stories)	15
Perpetrator made arrangements to mitigate personal/professional damage in case he/she was arrested for exfiltration-related behavior (e.g., obtained foreign passport, made travel plans)	16
Significant Life Events	
Perpetrator experienced an issue/event related to parental status that facilitated decision to exfiltrate resources (e.g., loss of custody)	0
Perpetrator experienced an issue/event related to marital/relationship status that facilitated decision to exfiltrate resources (e.g., divorce or adultery)	8
Perpetrator experienced an issue/event related to professional status that facilitated decision to exfiltrate resources (e.g., demotion)	20
Perpetrator experienced a personal loss that facilitated decision to exfiltrate resources (e.g., bankruptcy, death of a loved one)	4
Concerned Others	
Prior to arrest, someone noticed perpetrator's concerning behavior or a change in behavior	32

Overall, 65 out of the 83 perpetrators (78%) exhibited behavior that corresponded with at least one of the 10 behavioral threat assessment variables. As shown in Table 7, prior to their arrests, 21 out of the 83 perpetrators (25%) talked with at least one person who was neither an accomplice nor a handler about their exfiltration activity. Specifically, perpetrators talked with friends (n=10), professional colleagues (n=9), family members (n=3), and online acquaintances (n=3).

Perpetrators demonstrated concerning interests and engaged in planning behavior less often than they made concerning statements. Notably, only nine perpetrators infiltrated their victim organizations. That is, for the overwhelming majority of perpetrators (n=74), there was no evidence that they selected careers or took jobs with the intent to exfiltrate resources.

According to open source intelligence, the most common significant life event that contributed to the decision to exfiltrate resources related to the perpetrator's professional status. Twenty perpetrators (24%) experienced a predicating event related to work, such as a revoked clearance, a demotion, and/or denied leave requests.

Finally, in 32 out of the 83 cases (39%), open source intelligence revealed that someone noticed perpetrators' concerning behavior or a change in behavior prior to their arrest for resource exfiltration. In 23 of these 32 cases, someone went on to report what they had witnessed. There was no evidence that anyone reported a concern in the other nine cases.

FINDINGS & RECOMMENDATIONS

This study highlighted the fact that, other than being male, there is no demographic profile of employees who are most likely to exfiltrate DoD resources. Moreover, in line with previous insider threat research (Smith, Jaros, & Chandler, 2016), the overwhelming majority of perpetrators included in this project became malicious after they on-boarded with their victim organizations. Thorough background investigations, then, are just the start of a comprehensive security program. What follows is an overview of this project's major findings, along with corresponding recommendations to improve DoD's multi-layered strategy to detect, mitigate, and prevent future insider threats.

EXFILTRATION METHODS

User activity monitoring enables DoD to observe the electronic movement of its resources, but there appears to be insufficient protections against unauthorized physical movement. In this study, 65 out of the 83 perpetrators "collected or stored classified or other protected information at home or in any other unauthorized location." Of the 37 perpetrators for whom relevant open source intelligence was available, only 10 leveraged technology, such as email or fax, to move resources from an authorized to an unauthorized location. Instead, the majority physically walked resources out the door, either concealed on their bodies (i.e., pocket, under a hat) or in a container, such as a briefcase.

> **Recommendation #1:** Where possible, DoD should reduce the number of locations within a facility where critical electronic assets can be printed and/or physically reproduced. Then, DoD should institute random physical inspections, again when possible.

BEHAVIORAL INDICATORS

Although all 83 perpetrators (100%) engaged in some kind of behavior that corresponded with at least one of the 13 Adjudicative Guidelines, closer analysis revealed limited insight into potential intervention points prior to resource exfiltration. For example, 80 perpetrators "violated a written or recorded commitment made by the individual to the employer as a condition of employment." Similarly, 81 perpetrators "failed to comply with rules for the protection of classified or other protected information." Once a perpetrator has behaved in such a way that corresponds with either of these disqualifying factors, he/she likely has committed a serious crime associated with exfiltration, at which point it is likely too late to intervene.

In addition, some of the most commonly cited behavioral indicators for resource exfiltration appeared the least often among the perpetrators included in this study. For example, money was the most common motive, but the disqualifying factors associated with Adjudicative Guideline F: Financial Considerations yielded little to suggest the presence of financial pressures among the perpetrators. In other words, the financial motive did not appear to stem from debt but from greed.

In contrast with the Adjudicative Guidelines, experts designed the behavioral threat assessment framework specifically to identify and mitigate concerning behavior before it escalated. Sixty-five out of the 83 perpetrators exhibited behavior that corresponded with at least one of the 10 behavioral threat assessment variables included in this study. For example, nearly one-quarter of all perpetrators (n=21) talked specifically about their exfiltration activities to someone who was neither a handler nor an accomplice. In 32 of the cases, someone noticed a change in behavior or concerning behavior prior to the perpetrator's arrest, and of those, 23 cases involved someone who witnessed something and went on to report what they saw.

> **Recommendation #2:** DoD should integrate best practices for behavioral threat assessment into the insider threat training mandated by the *National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs* for both Insider Threat Program Personnel (Section F) and the general workforce (Section I).

PROFESSIONAL STRESSORS

Employees who experience professional stressors, such as a demotion, could target DoD for retaliation against perceived wrongs. In this study, nearly one-quarter of all perpetrators experienced an issue or event related to their professional status that facilitated the decision to exfiltrate resources. Moreover, behind money and ideology, a desire for revenge and a desire to improve one's career were the most common motives for resource exfiltration. These results emphasize the importance for supervisors, commanders, and Human Resources personnel to respond to problematic behavior with care and consideration, so as not to endanger the future welfare of DoD or its resources.

> **Recommendation #3:** DoD should ensure that its personnel who issue disciplinary notices are trained in conflict resolution and/or de-escalation strategies, and security personnel should be on hand to ensure those who are terminated do not retain physical or logical access. DoD also should prioritize additional research to identify best practices to reintegrate employees into the workforce after serious disciplinary action, such as a demotion or suspension. Together with wellness programs such as Employee Assistance Programs, these practices should help to ensure employees successfully recover from difficult events and situations.

LIMITATIONS

This project is limited by its scope and its data sources. First, this project only includes cases in which a perpetrator exfiltrated a DoD resource, which limits its generalizability to other government agencies and to the private sector. Second, researchers relied entirely on open source intelligence, which is often incomplete to protect investigative tactics, techniques, and procedures. Moreover, the accuracy and completeness of open source intelligence tends to evolve over time as court proceedings supplant speculation.

FUTURE RESEARCH

Future research should broaden the eligibility criteria to include non-DoD resources. Also, if possible, future studies should incorporate official records such as perpetrators' personnel files, investigative files, and trial transcripts. While the resulting reports likely would be restricted to certain audiences, these records could serve to validate or correct current findings and identify additional intervention points.

The findings from this project also give rise to a number of research questions worthy of future study. For example, behind money, ideology was the most common motive for resource exfiltration. Although radicalization is often studied in reference to future violence, it might apply to ideologically driven, non-violent perpetrators. Additional research questions include, but are not limited to:

- Were any perpetrators investigated for a higher clearance after their exfiltration had begun? If so, did perpetrators have to take active measures to conceal their exfiltration activity or was the investigation too narrow to recognize potential behavioral indicators?
- Ten perpetrators included in this study intentionally memorized information for later unauthorized transmission, but others just leveraged what they had learned during the course of their job duties long after they lost access. That is, they transmitted resources they happened to remember. How can DoD continue to protect its resources after personnel have left DoD?
- In 32 of the cases, someone noticed a change in behavior or concerning behavior prior to the perpetrator's arrest. Of these 32, someone went on to report what they had seen in 23 of the cases. At the individual level, was there a qualitative difference in the types of behavior or behavior changes that people went on to report versus those they did not? At the organizational levels, were there factors that impeded reporting, such as unclear or absent policies and corresponding standard operating procedures?

REFERENCES

American Psychological Association. (2013). Gun violence: Prediction, prevention, and policy. Retrieved from http://www.apa.org/pubs/info/reports/gunviolence-prevention.aspx

Bhattacharjee, Y. (2016, October). The spy who couldn't spell: How the biggest heist in the history of US espionage was foiled. *The Guardian.*

Borum, R., Fein, R., Vossekuil, B., & Berglund, J. (1999). Threat Assessment: Defining an approach for evaluating risk of targeted violence. Behavioral Sciences & the Law. Vol. 17, No. 3, 323-337. John Wiley & Sons, Ltd.

Bush, G. (December 29, 2005). Presidential memorandum - Adjudicative Guidelines. Washington D.C.

Commission to Review DoD Security Policy and Practices. (1985). *Keeping the Nation's Secrets: A Report to the Secretary of Defense.* Retrieved from https://fas.org/sgp/library/stilwell.html

Fein, R. A., & Vossekuil, B. (1997). *Preventing assassination: Secret Service Exceptional Case Study Project (NCJ 167224).* Washington, DC: U.S. Dept. of Justice, Office of Justice Programs, National Institute of Justice.

The MITRE Corporation. (2009). *Rare events* (organization report number JSR-09-108).

Nakashima, E. (2016, October). Government alleges former NSA contractor stole 'astonishing quantity' of classified material over 20 years. *The Washington Post.*

Nakashima, E. & Zapotosky, M. (2016, October). NSA contractor thought to have taken classified material the old-fashioned way. *The Washington Post.*

Office of the Director of National Intelligence. (2012). *National insider threat policy and minimum standards for Executive Branch insider threat programs* [Presidential Memorandum]. Retrieved from https://www.dni.gov/index.php/ic-legal-reference-book/presidential-memorandum-nitp-minimum-standards-for-insider-threat-program

Popkin, J. (2013, April). Ana Montes did much harm spying for Cuba. Chances are, you haven't heard of her. *The Washington Post.*

Shaw, E.D., & Fischer, L.F. (2005). *Ten tales of betrayal: The threat to corporate infrastructures by information technology insiders - Report 1 - Overview and general observations* (TR 05-04). Monterey, CA: Defense Personnel Security Research Center. (For Official Use Only). DTIC: ADB308475

Smith, C.M., Jaros, S.L., & Chandler, C.J. (2016). Foreground factors of DoD workplace homicide: A comparative case analysis of incidents between 2009-2015. (TR 17-01). Seaside, CA: Defense Personnel and Security Research Center/Office of People Analytics. (For Official Use Only). DTIC: AD1036694

APPENDIX A: DISQUALIFYING FACTORS FOR THE ADJUDICATIVE GUIDELINES

The following table presents the list of the 75 disqualifying factors associated with the 13 Adjudicative Guidelines. The counts indicate the total number of perpetrators whose behavior matched each disqualifying factor prior to arrest. The italicized text is text added to the disqualifying factor for clarification purposes for this project.

Table 8
Perpetrator Pre-Arrest Behavior Categorized by Disqualifying Factor, Full Results*

ADJUDICATIVE GUIDELINE & DISQUALIFYING FACTOR	COUNT
GUIDELINE A: ALLEGIANCE TO THE UNITED STATES	
Person associated with or sympathized with persons who attempted to commit or who committed any act of sabotage, espionage, treason, terrorism, or sedition against the United States. *Do not include a person's handler or anyone posing as a handler.*	20
Person associated with or sympathized with persons or organizations that advocated, threatened, or used force or violence, or used any other illegal or unconstitutional means to overthrow the government, prevent government personnel from performing their duties, gain retribution for perceived wrongs caused by the government, or prevent others from exercising their rights under the Constitution or laws. *Do not include a person's handler or anyone posing as a handler.*	7

GUIDELINE B: FOREIGN INFLUENCE	
Person had contact with a foreign family member, business or professional associate, friend, or other person who was a citizen of or resident in a foreign country, which could have created a heightened risk of foreign exploitation, inducement, manipulation, pressure, or coercion. *Include all countries regardless of relationship with the United States. Do not include a person's handler or anyone posing as a handler.*	44
Person had connections to a foreign person, group, or government that could have created a potential conflict of interest between the individual's obligation to protect sensitive information or technology and the individual's desire to help a foreign person, group, or country by providing that information. *Include all countries regardless of relationship with the United States. Do not include a person's handler or anyone posing as a handler.*	40
Person shared living quarters with a person or persons, regardless of citizenship status, which could have created a heightened risk of foreign inducement, manipulation, pressure, or coercion. *Include all countries regardless of relationship with the United States.*	15
Person had a substantial business, financial, or property interest in a foreign country, or in any foreign-owned or foreign-operated business, which could have subjected the individual to heightened risk of foreign influence or exploitation. *Include all countries regardless of relationship with the United States.*	8
Person failed to report, when required, association with a foreign national, *to include a person's handler or anyone posing as a handler. Include all countries regardless of relationship with the United States.*	42
Person had an unauthorized association with a suspected or known agent, associate, or employee of a foreign intelligence service, *to include a person's handler or anyone posing as a handler. Include all countries regardless of relationship with the United States*	38
There were indications that representatives or nationals from a foreign country acted to increase the person's vulnerability to possible future exploitation, inducement, manipulation, pressure, or coercion. *Include all countries regardless of relationship with the United States.*	6
Person engaged in conduct, especially while traveling outside the U.S., which may have made the individual vulnerable to exploitation, pressure, or coercion by a foreign person, group, government, or country.	11
GUIDELINE C: FOREIGN PREFERENCE	
Person exercised any right, privilege or obligation of foreign citizenship after becoming a U.S. citizen or through the foreign citizenship of a family member. This includes, but is not limited to: - Possessed a current foreign passport; - Military service or a willingness to bear arms for a foreign country; - Accepted educational, medical, retirement, social welfare, or other such benefits from a foreign country; - Residence in a foreign country to meet citizenship requirements; - Used foreign citizenship to protect financial or business interests in another country; - Sought or held political office in a foreign country; or - Voted in a foreign election.	8
Person performed or attempted to perform duties, or otherwise acted, so as to serve the interests of a foreign person, group, organization, or government in conflict with the National security interest.	71
Person made any statement or action that showed allegiance to a country other than the United States (*e.g.,* declaration of intent to renounce United States citizenship or renunciation of United States citizenship; plans to defect).	19

GUIDELINE D: SEXUAL BEHAVIOR	
Person engaged in sexual behavior of a criminal nature (i.e., civilian or military), whether or not the individual was prosecuted.	7
Person demonstrated a pattern of compulsive, self-destructive, or high-risk sexual behavior that the person was unable to stop or that may have been symptomatic of a personality disorder.	1
Person engaged in sexual behavior that could have caused an individual to be vulnerable to coercion, exploitation, or duress.	8
Person engaged in sexual behavior of a public nature and/or that reflected lack of discretion or judgment.	3
GUIDELINE E: PERSONAL CONDUCT	
Person engaged in untrustworthy or unreliable behavior to include breach of client confidentiality, release of proprietary information, unauthorized release of sensitive corporate or other government-protected information.	79
Person engaged in disruptive, violent, or other inappropriate behavior in the workplace.	7
Other than resource exfiltration, person engaged in a pattern of dishonesty or rule violations *(i.e., history of performance issues).*	15
Person misused government or other employer's time or resources *(i.e., personnel, facilities, accesses, equipment).*	65
While in another country, person engaged in any activity that was illegal in that country or that was legal in that country but illegal in the United States and could have served as a basis for exploitation or pressure by the foreign security or intelligence service or other group.	7
Person violated a written or recorded commitment made by the individual to the employer as a condition of employment.	80
Person associated with persons involved in criminal activity.	20
GUIDELINE F: FINANCIAL CONSIDERATIONS	
Person demonstrated an inability or unwillingness to satisfy debts.	9
Person's was in debt because of frivolous or irresponsible spending and the absence of any evidence of willingness or intent to pay the debt or establish a realistic plan to pay the debt.	7
Person had a history of not meeting financial obligations.	7
Person had a history of deceptive or illegal financial practices such as embezzlement, employee theft, check fraud, income tax evasion, expense account fraud, filing deceptive loan statements, and other intentional financial breaches of trust.	7
Person consistently spent beyond his/her means, which may be indicated by excessive indebtedness, significant negative cash flow, high debt-to-income ratio, and/or other financial analysis.	7
Person had financial problems linked to drug abuse, alcoholism, gambling problems, or other issues of security concern.	5
Person failed to file annual Federal, state, or local income tax returns as required or fraudulently filed any of the same.	3
Person demonstrated unexplained affluence, as shown by a lifestyle or standard of living, increase in net worth, or money transfers that could not be explained by known legal sources of income.	8
Person demonstrated compulsive or addictive gambling as indicated by an unsuccessful attempt to stop gambling, "chasing losses" (i.e., increasing the bets or returning another day in an effort to get even), concealment of gambling losses, borrowing money to fund gambling or pay for gambling.	1

GUIDELINE G: ALCOHOL CONSUMPTION	
Person had alcohol-related incidents away from work, such as driving while under the influence, fighting, child or spouse abuse, disturbing the peace, or other incidents of concern, regardless of whether the individual was diagnosed as an alcohol abuser or alcohol dependent.	3
Person had alcohol-related incidents at work, such as reporting for work or duty in an intoxicated or impaired condition, or drinking on the job, regardless of whether the individual was diagnosed as an alcohol abuser or alcohol dependent.	1
Person had a history of habitual or binge consumption of alcohol to the point of impaired judgment, regardless of whether the individual was diagnosed as an alcohol abuser or alcohol dependent.	9
Person was diagnosed by a duly qualified medical professional (*e.g.,* physician, clinical psychologist, or psychiatrist) with alcohol abuse or alcohol dependence.	2
Person was evaluated for alcohol abuse or alcohol dependence by a licensed clinical social worker who was a staff member of a recognized alcohol treatment program.	1
Person relapsed after a diagnosis of alcohol abuse or dependence and completion of an alcohol rehabilitation program.	1
Person failed to follow any court order regarding alcohol education, evaluation, treatment, or abstinence.	0
GUIDELINE H: DRUG INVOLVEMENT	
Person demonstrated any type of drug abuse.	8
Person tested positive for illegal drug use.	1
Person possessed illegal drugs, including cultivation, processing, manufacture, purchase, sale, or distribution; or possession of drug paraphernalia.	11
Person was diagnosed by a duly qualified medical professional (*e.g.,* physician, clinical psychologist, or psychiatrist) with drug abuse or drug dependence.	0
Person was evaluated for drug abuse or drug dependence by a licensed clinical social worker who was a staff member of a recognized drug treatment program.	0
Person failed to successfully complete a drug treatment program prescribed by a duly qualified medical professional.	0
Person used any illegal drug after being granted a security clearance.	5
Person expressed intent to continue illegal drug use, or failed to clearly and convincingly commit to discontinue drug use.	4
GUIDELINE I: PSYCHOLOGICAL CONDITIONS	
Person engaged in behavior that cast doubt on his/her judgment, reliability, or trustworthiness that was not covered under any other guideline, including, but not limited to, emotionally unstable, irresponsible, dysfunctional, violent, paranoid, or bizarre behavior.	16
A duly qualified mental health professional opined that the individual had a condition not covered under any other guideline that may have impaired judgment, reliability, or trustworthiness.	9
The individual failed to follow treatment advice related to a diagnosed emotional, mental, or personality condition (*e.g.,* failure to take prescribed medication).	1

GUIDELINE J: CRIMINAL CONDUCT	
Other than resource exfiltration, person committed a single serious crime or multiple lesser offenses (i.e., criminal record).	13
Person was discharged or dismissed from the Armed Forces under dishonorable conditions.	1
Person had an allegation or admission of criminal conduct (i.e., civilian or military), regardless of whether the person was formally charged, formally prosecuted or convicted.	24
Person was ever on parole or probation.	0
Person violated parole or probation, or failed to complete a court-mandated rehabilitation program.	0
GUIDELINE K: HANDLING PROTECTED INFORMATION	
Person engaged in deliberate or negligent disclosure of classified or other protected information to unauthorized persons, including, but not limited to, personal or business contacts, to the media, or to persons present at seminars, meetings, or conferences.	74
Person collected or stored classified or other protected information at home or in any other unauthorized location.	65
Person loaded, drafted, edited, modified, transmitted, or otherwise handled classified reports, data, or other protected information on any unapproved equipment including, but not limited to, any typewriter, word processor, or computer hardware, software, drive, system, gameboard, handheld, “palm” or pocket device or other adjunct equipment.	29
Person made an inappropriate effort to obtain or view classified or other protected information outside his/her need to know.	27
Person copied classified or other protected information in a manner designed to conceal or remove classification or other document control markings.	9
Person viewed or downloaded protected information from a secure system when the protected information was beyond his/her need-to-know.	10
Person failed to comply with rules for the protection of classified or other protected information.	81
Person practiced negligent or lax security habits *related to handling protected information* that persisted despite counseling by management.	4
Other than resource exfiltration, person failed to comply with rules or regulations that resulted in damage to the National security, regardless of whether it was deliberate or negligent *(i.e., history of security violations).*	1
GUIDELINE L: OUTSIDE ACTIVITIES	
Person engaged in any legitimate employment or service, whether compensated or volunteer, with: - The government of a foreign country; - Any foreign national, organization, or other entity; - A representative of any foreign interest; or - Any foreign, domestic, or international organization or person engaged in analysis, discussion, or publication of material on intelligence, defense, foreign affairs, or protected technology.	6
Person failed to report or fully disclose a legitimate employment or service activity when this was required.	2

GUIDELINE M: USE OF INFORMATION TECHNOLOGY SYSTEMS	
Person illegally or without authorization entered into any information technology system or component thereof.	6
Person illegally or without authorization modified, destroyed, manipulated or denied access to protected information, software, firmware, or hardware in an information technology system.	2
Person used any information technology system to gain unauthorized access to another system or to a compartmented area within the same system.	4
Person downloaded, stored, or transmitted classified information on or to any unauthorized software, hardware, or information technology system.	22
Person used a government or other information technology system without authorization.	6
Person introduced, removed, or duplicated hardware, firmware, software, or media to or from any information technology system without authorization, when prohibited by rules, procedures, guidelines, or regulations.	10
Person practiced negligent or lax security habits in handling information technology that persisted despite counseling by management.	0
Other than resource exfiltration, person misused information technology, whether deliberate or negligent, that resulted in damage to the national security *(i.e., history of misuse).*	1

* Italicized text added to the disqualifying factor for clarification purposes for this project.

APPENDIX B: DATE EXFILTRATION BEGAN

T1. DATE OF FIRST UNAUTHORIZED POSSESSION *(DATE)*

For all perpetrators, the earliest date on which the person was known to possess protected information without authorization, MM/DD/YYYY. This includes when the person first accessed protected information without a need-to-know or took protected information home without authorization. Enter 88/88/8888 if person never possessed protected information without authorization.

T2. DATE OF FIRST VOLUNTEER (*DATE*)

For perpetrators who volunteered, the earliest known date on which the person attempted – successfully or unsuccessfully – to contact a potential unauthorized recipient, MM/DD/YYYY. This includes contact with a named individual and/or general outreach to a foreign country, publication, or group. Enter 77/77/7777 if there is not enough information to determine whether or not the person was a volunteer. Enter 88/88/8888 if person did not volunteer to commit resource exfiltration.

T3. Volunteer Response (*Date*)

For perpetrators who volunteered, the earliest known date on which the person received a response from a potential unauthorized recipient, MM/DD/YYYY. **This excludes any response from an undercover agent.** Enter 77/77/7777 if there is not enough information to determine whether or not the person was a volunteer. Enter 88/88/8888 if person did not volunteer to commit resource exfiltration or never received a response from an unauthorized recipient.

T4. Volunteer Transmission (*Date*)

For perpetrators who volunteered, the earliest date on which the person attempted to transmit – successfully or unsuccessfully – protected information to an unauthorized recipient, MM/DD/YYYY. **This excludes any transmission to an undercover agent.** Enter 77/77/7777 if there is not enough information to determine whether or not the person was a volunteer. Enter 88/88/888 if person did not attempt to transmit protected information or only transmitted protected information to an undercover agent.

T5. DATE OF FIRST RECRUITMENT (*DATE*)

For perpetrators who were recruited, the earliest known date on which the person met an unauthorized recipient, MM/DD/YYYY. **This excludes any meetings with an undercover agent.** Enter 77/77/7777 if there is not enough information to determine whether or not the person was a recruit. Enter 88/88/8888 if person was not recruited to commit resource exfiltration or only recruited by an undercover agent.

T6. Recruitment Request (*Date*)

For perpetrators who were recruited, the earliest known date on which the person received a request for protected information from an unauthorized recipient, MM/DD/YYYY. **This excludes any request from an undercover agent.** Enter 77/77/7777 if there is not enough information to determine whether or not the person was a recruit. Enter 88/88/8888 if person was not recruited to commit resource exfiltration or only recruited by an undercover agent.

T7. Recruitment Transmission (*Date*)

For perpetrators who were recruited, the earliest known date on which the person attempted to transmit – successfully or unsuccessfully – protected information to an unauthorized recipient, MM/DD/YYYY. **This excludes any transmission to an undercover agent.** Enter 77/77/7777 if there is not enough information to determine whether or not the person was a recruit. Enter 88/88/888 if person did not attempt to transmit protected information or only transmitted protected information to an undercover agent.

T8. DATE OF FIRST STING (*DATE*)

For perpetrators who were involved in a sting operation, the earliest known date on which the person came to the attention of investigators, MM/DD/YYYY. Enter 88/88/8888 if person was not involved in a sting operation.

T9. Sting Request (*Date*)

For perpetrators who were involved in a sting operation, the earliest known date on which the person was contacted by an undercover agent, MM/DD/YYYY. Enter 88/88/8888 if person was not involved in a sting operation.

T10. Sting Transmission (*Date*)

For perpetrators who were involved in a sting operation, the earliest known date on which the person attempted to transmit – successfully or unsuccessfully – protected information to an undercover agent, MM/DD/YYYY. Enter 88/88/888 if person did not attempt to transmit protected information to an undercover agent.

T11. DATE EXFILTRATION BEGAN (***DATE***)

Earliest known date among variables T1 – T10, MM/DD/YYYY. **This variable cannot be missing.**