NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

UNAUTHORIZED DISCLOSURE: CAN BEHAVIORAL INDICATORS HELP PREDICT WHO WILL COMMIT UNAUTHORIZED DISCLOSURE OF CLASSIFIED NATIONAL SECURITY INFORMATION?

by

Karen Elizabeth Sims

June 2015

Thesis Co-Advisors: Robert Simeral
Kathleen Kiernan

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704–0188

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** June 2015	**3. REPORT TYPE AND DATES COVERED** Master's Thesis

4. TITLE AND SUBTITLE
UNAUTHORIZED DISCLOSURE: CAN BEHAVIORAL INDICATORS HELP PREDICT WHO WILL COMMIT UNAUTHORIZED DISCLOSURE OF CLASSIFIED NATIONAL SECURITY INFORMATION?

5. FUNDING NUMBERS

6. AUTHOR(S) Karen Elizabeth Sims

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES)
N/A

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB protocol number ____N/A____.

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited

12b. DISTRIBUTION CODE
A

13. ABSTRACT (maximum 200 words)

Federal government security-cleared personnel have been disclosing federal government classified national security information, whether to a foreign government or the United States media, at an increasing rate since the 1980s. Can common personal or psychological characteristics or motivations be identified from historical cases that could indicate the likelihood of a current or potential federal employee to disclose national security information without authorization? Reasons for unauthorized disclosure range from financial, to "whistle-blowing," to a desire to change international policy, to sympathy and strong ties with a foreign government. The focus of this research is on the behavioral characteristics that are similar or different between known, studied historical cases of personnel associated with the federal government who have disclosed classified information without authorization. Upon review of existing data, the prevalent behavioral characteristic of the cases is one of a disgruntled employee (*ideology/ disillusionment/loyalty*). A disgruntled employee becomes the largest concern as an insider threat, one who is willing to compromise his or her feelings of loyalty to the organization and the nation for a myriad of reasons.

14. SUBJECT TERMS
insider threat, unauthorized disclosure, classified national security information, behavioral indicators, ideology, disillusionment, loyalty, intelligence community culture, Aldrich Ames, Robert Hansson, Chelsea (Bradley) Manning, Edward Snowden, whistleblower, espionage, spy, patriot, traitor, Central Intelligence Agency, Federal Bureau of Investigations, Department of Defense, financial gain, loyalty, trustworthiness, character, reliability, security clearance, adjudicative guidelines, continuous evaluation

15. NUMBER OF PAGES
153

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	UU

NSN 7540–01-280-5500

Standard Form 298 (Rev. 2–89)
Prescribed by ANSI Std. 239–18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

UNAUTHORIZED DISCLOSURE: CAN BEHAVIORAL INDICATORS HELP PREDICT WHO WILL COMMIT UNAUTHORIZED DISCLOSURE OF CLASSIFIED NATIONAL SECURITY INFORMATION?

Karen Elizabeth Sims
Senior Security Specialist, Department of Homeland Security,
Office of the Chief Security Officer, Washington, DC
B.A., Luther College, 1993
M.A., Montclair State University, 2005

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)**

from the

**NAVAL POSTGRADUATE SCHOOL
June 2015**

Author: Karen Elizabeth Sims

Approved by: Robert Simeral
Thesis Co-Advisor

Kathleen Kiernan
Thesis Co-Advisor

Mohammed Hafez
Chair, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Federal government security-cleared personnel have been disclosing federal government classified national security information, whether to a foreign government or the United States media, at an increasing rate since the 1980s. Can common personal or psychological characteristics or motivations be identified from historical cases that could indicate the likelihood of a current or potential federal employee to disclose national security information without authorization? Reasons for unauthorized disclosure range from financial, to "whistle-blowing," to a desire to change international policy, to sympathy and strong ties with a foreign government. The focus of this research is on the behavioral characteristics that are similar or different between known, studied historical cases of personnel associated with the federal government who have disclosed classified information without authorization. Upon review of existing data, the prevalent behavioral characteristic of the cases is one of a disgruntled employee (*ideology/ disillusionment/loyalty*). A disgruntled employee becomes the largest concern as an insider threat, one who is willing to compromise his or her feelings of loyalty to the organization and the nation for a myriad of reasons.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

ACES	Automated Continuous Evaluation System
AEC	Atomic Energy Commission
CAF	Central Adjudications Facility
CCF	Central Clearance Facility
CE	continuous evaluation
CEP	Continuous Evaluation Program
CERT	Computer Emergency Readiness Team
CIA	Central Intelligence Agency
CME	Continuous Monitoring and Evaluation
CRS	Congressional Research Service
DA	Department of Army
DC	District of Columbia
DCI	Director of Central Intelligence
DIA	Defense Intelligence Agency
DCII	Defense Central Index of Investigations
DIS	Defense Investigative Service
DHS	Department of Homeland Security
DNI	Director of National Intelligence
DOD	Department of Defense
DOE	Department of Energy
DOJ	Department of Justice
DoN	Department of Navy
DSS	Defense Security Service
E.O.	executive order
FBI	Federal Bureau of Investigation
GAO	Government Accountability Office
GWOT	global war on terror
HQ	headquarters
IC	Intelligence Community
ICD	Intelligence Community Directive
INSA	Intelligence and National Security Alliance
ISCAP	Interagency Security Classification Appeals Panel

ISOO	Information and Oversight Office
IT	information technology
KGB	Komitet gosudarstvennoy bezopasnosti (Soviet Union Intelligence Agency)
NATO	North Atlantic Treating Organization
NCSC	National Counterintelligence and Security Center
NDC	National Declassification Center
NISC	Naval Intelligence Support Center
NRO	National Reconnaissance Office
NSA	National Security Agency
ODNI	Office of the Director of National Intelligence
OMB	Office of Management and Budget
ONCI	Office of National Counterintelligence
OPM	Office of Personnel Management
PERSEREC	Defense Personnel and Security Research Center
PII	Personally Identifiable Information
PLO	Palestine Liberation Organization
PPD	presidential policy directive
PR	periodic review
PSI	personnel security investigation
PSP	Personnel Security Program
SAP	Special Access Program
SCI	Sensitive Compartmented Information
SF	standard form
SIT	social identity theory
TEE	training and education and evaluation of training effectiveness
TSA	Transportation Security Authority
U.S.	United States
USCG	United States Coast Guard
USMC	United States Marine Corps
USS	United States ship
VA	United States Department of Veterans Affairs

EXECUTIVE SUMMARY

Federal government security-cleared personnel have been disclosing federal government classified national security information, whether to a foreign government or the United States media, at an increasing rate since the 1980s. Can common personal or psychological characteristics or motivations be identified from historical cases that could indicate the likelihood of a current or potential federal employee to disclose national security information without authorization? Executive Order 13526, Classified National Security Information, states, "National defense has required that certain information be maintained in confidence in order to protect our citizens, our democratic institutions, our homeland security and our interactions with foreign nations."[1] In order to access classified national security information, an individual must have a "need-to-know," or the need to have access to information to perform official duties. If it is determined he/she has a need to know, that person must undergo a background investigation to determine loyalty, trustworthiness, and reliability, as well as sign U.S. Government Standard Form 312, Classified Information Nondisclosure Agreement. Recent unauthorized disclosures of classified information have caused outrage on Capitol Hill and eroded the American peoples' confidence in the security clearance process. While such recent disclosures by Edward Snowden and Chelsea (formerly Bradley) Manning highlight recent incidents, there is a history of unauthorized disclosure of classified information going back to our nation's very beginning.

Why do people disclose information with which they have been entrusted? Reasons for unauthorized disclosure range from financial, to "whistle-blowing," to a desire to change international policy, to sympathy and strong ties with a foreign government. The focus of this research is on the behavioral characteristics that are similar or different between known, studied historical cases of personnel associated with the federal government who have disclosed classified information without authorization. Cases studied include Aldrich Ames, Ana Belen Montes, Chelsea (Bradley) Manning,

[1] Exec. Order No. 13526, 75 Fed. Reg. 2 (Jan. 5, 2010), https://www.whitehouse.gov/the-press-office/executive-order-classified-national-security-information, 707.

Brian Regan, Bryan Underwood, Greg William Bergersen, Hassan Abu-Jihaad (Paul R. Hall), Robert Hanssen, John Walker, Jonathon Pollard and Edward Snowden. Selection is based on unauthorized disclosure since the 1980s, including 1985—referred to as the "year of the spy."

Upon review of existing data, the prevalent behavioral characteristic of the cases (10 out of 11 cases) is one of a disgruntled employee (*ideology/disillusionment/loyalty*). A disgruntled employee becomes the largest concern of insider threat, one who is willing to compromise his or her feelings of loyalty to the organization and the nation for a myriad of reasons. While personal security background investigations review information from the present to up to 10 years prior,

> Studies of espionage based on personal interviews with offenders suggest a pattern in which personal disruptions or crises precede, or "trigger," an individual's decision to commit espionage. Crises could be positive or negative, and include divorce, death, starting a new relationship, or exhibiting radically changed behavior. Commentators have speculated that if help or timely intervention had been offered in these cases, the crime might have been averted.[2]

Thus,

> Assessing the quality of a person's moral development at an early life stage may be irrelevant to the context of later action when unforeseen events create a condition of personal strain for which trust violation would be a possible resolution.[3]

There is no way to determine how many potential spies or persons bent on disclosing classified information were eliminated through the vetting of data collected during the initial security clearance request process. What is depicted in this thesis is the result of employees who passed the screening process and were fully trusted to perform their duties. The conclusion to be drawn from this is two-fold. First, first- and second-line managers of employees who have access to classified information must be keenly aware

---

[2] Katherine L. Herbig, *Changes in Espionage by Americans: 1947–2007*, Department of Defense Technical Report 08–05 (Monterey, CA: Defense Personnel Security Research Center, 2008), http://www.dhra.mil/perserec/reports/tr08-05.pdf, xi.

[3] Theodore R. Sarbin, Ralph M. Carney, and Carson Eoyang, eds. *Citizen Espionage: Studies in Trust and Betrayal* (Westport, CT: Praeger, 1994), 119.

of any changes in the personality of their employees. They must go beyond simply giving work assignments and grading results. They have to be able to read slight changes in attitude, performance, personality, and be prepared to make tough decisions about taking positive action when nuances, however slight, are detected. Because intellect and ego play an important part in employee performance, the manager must be trained to deal with employees whose behavior is outside the norm in those regards. Second, managers must, on a regular basis, encourage all employees to be mindful of personality or lifestyle changes of fellow employees and provide a protected avenue for them to discuss fellow employee behavior. “See something, say something” is a phrase that belongs in the work place and applies to both personality and material things. Recognizing and dealing with disgruntled employees might just prevent or mitigate unauthorized disclosure. Disgruntlement leads to changes in ideology, disillusionment with one’s organization, and ultimately may change national loyalty; the predominant factors of which supervisors must be aware.

A continuing evaluation system fits hand in glove with managerial awareness of and peer recognition of behavioral or drastic character changes in employees. Formally, there is nothing between the initial screening process and a periodic review (after five or 10 years depending on the classification level). A continuing evaluation system would retrieve real-time data from a variety of sources to determine those employees whose lifestyle or behavior might have changed.

Finally, the government must institute a process of routinely reviewing classified positions to determine those positions that no longer have security clearances required. The fewer classified positions, the fewer employees have access to classified information. That lessens the opportunity for unauthorized disclosure and drastically reduces the strain on the entire security clearance process.

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

Dedicated to my husband, Douglas Arthur, whose love and constant encouragement and support led me to completion.

And to my brother, Christopher Paul, I wish you were here to share this accomplishment with me.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. THESIS QUESTION

Federal government security-cleared personnel are disclosing federal government classified national security information, whether to a foreign government or the United States (U.S.) media at an increasing rate since the 1980s. According to Heuer and Herbig:

> Five spies were arrested or otherwise publicly exposed during the decade of the 1950s. This increased to 13 in the 1960s and 13 in the 1970s, respectively. Arrests and other public exposures mushroomed to 56 in the 1980s and remained at a high level, with 29, in the 1990s.[4]

Can common personal or psychological characteristics or motivations be identified from historical cases that could indicate the likelihood of a current or potential federal employee to disclose national security information without authorization?

B. IMPORTANCE OF QUESTION BEING ANSWERED

Executive Order (E.O.) 13526, Classified National Security Information, states, "…national defense has required that certain information be maintained in confidence in order to protect our citizens, our democratic institutions, our homeland security and our interactions with foreign nations."[5] In order to access classified national security information, an individual must have a "need-to-know," or the need to have access to information in order to perform official duties. If it is determined he/she has a need to know, that person must undergo a background investigation to determine loyalty, trustworthiness and reliability, as well as sign a U.S. government Standard Form (SF) 312, Classified Information Nondisclosure Agreement. Recent unauthorized disclosures of classified information have caused outrage on Capitol Hill and eroded the American peoples' confidence in the security clearance process. While such recent disclosures by Chelsea (formerly Bradley) Manning and Edward Snowden highlight recent incidents, there remains a history of unauthorized disclosure of classified information going back to

[4] Richards J. Heuer, and Katherine Herbig, *Espionage by the Numbers: A Statistical Overview*, accessed April 14, 2015, http://www.wright.edu/rsp/Security/Treason/Numbers.htm

[5] Exec. Order No. 13526, 707.

our nation's very beginning, becoming more significant during World War II and the creation of the atomic bomb[6] and exploding during the 1980s, known as the decade of the spy.

While Congress and the public clamor for greater accountability and oversight of the security clearance program, this may not be realistic given the changed and changing conditions of an increasingly decentralized workforce and declines in hiring. The federal government continues toward a more mobile workforce, working via telework or remote work sites, partly as a result of the seemingly constant reduction in agency budgets, as well as long, time-consuming commutes. With more outside distractions and less direct human interaction, it would appear that knowledge of co-workers' habits would decrease and lead to less oversight. Self-reporting of violations significant to holding a clearance reinforces the responsibilities and roles of the security clearance holder, but with what frequency do employees relay dramatic changes in their lives, for example, attempts to overthrow the U.S. government, bankruptcy, arrests for misdemeanors, or misuse of government information systems? By the very nature of the requirement to self-report, my experience is that it is rarely done. In fact, in almost nine years of government service, I do not know of a single case where a fellow employee reported he or she was declaring bankruptcy, using illegal drugs, involved in any type of skullduggery, et cetera.

However, with the current culture of people willingly posting personal information online, persons could unwittingly self-report. Such innocent postings could include pictures taken on a trip overseas where the person is clearly engaging foreign nationals; or perhaps that casual picture taken at a beach party that shows the person is inebriated and perhaps a few "joints" lying around, or a casual comment about not being able to make a mortgage payment. While these postings are on the Internet, one could argue they are not public, but rather intended for viewing by "friends" or "contacts" of the poster. That then presents a dilemma for those friends and contacts who are

[6] During the course of the Manhattan Project, counterintelligence agents "handled more than 1,000 general subversive investigations, over 1,500 cases in which classified project information was transmitted to unauthorized persons, approximately 100 suspected espionage cases, and approximately 200 suspected sabotage cases." *Manhattan District History, Security Information Book I-General, Volume 14-Intelligence and Security*, September 26, 1952, Federation of American Scientists, http://fas.org/sgp/library/mdhist-vol14.pdf, S2-3.

government employees and are expected to report such violations. New technologies, such as the Department of Defense (DOD) Automated Continuous Evaluation System (ACES), can be used to discover identifiable behavioral or personality characteristics that could be indicative of an individual who may disclose classified national security information without authorization. Existing and future technology should be used to gather open source information, aligning with the "whole person" concept.[7]

Why do people disclose information with which they have been entrusted? Reasons for unauthorized disclosure range from financial, to "whistle-blowing," to a desire to change international policy, to sympathy and strong ties with a foreign government. The focus of this research will be the behavioral characteristics that are similar or different between known, studied historical cases of personnel associated with the federal government who have disclosed classified information without authorization. If common characteristics or motivations can be identified, the security clearance process may be better equipped to recognize those current or future employees who might compromise their country for their own personal gain.

C. DESCRIPTION OF RESEARCH METHOD USED

The focus of this research is the observable behavioral characteristics that are similar or different between known, studied historical cases of U.S. personnel associated with the federal government who have disclosed classified national security information without authorization. This thesis provides a comprehensive list of identifiable character traits of persons involved in historical cases of leaking information, including a ranking of the characteristics from most to least common. It is expected that the behavioral characteristics will fall under the 13 adjudicative guidelines established by the Office of

[7] In relationship to the 13 adjudicative guidelines, the whole-person concept takes into account nine factors, often referred to as "General Criteria," that must be considered with the adjudicative guidelines. The nine factors are, "1) the nature, extent, and seriousness of the conduct; 2)the circumstances surrounding the conduct, to include knowledgeable participation; 3)the frequency and recentcy of the conduct; 4)the individual's age and maturity at the time of the conduct; 5)the extent to which participation is voluntary; 6)the presence or absence of rehabilitation and other permanent behavioral changes; 7)the motivation for the conduct; 8)the potential for pressure, coercion, exploitation, or duress; and 9)the likelihood of continuation or recurrence." U.S. Department of State, *Adjudicative Guidelines for Determining Eligibility for Access to Classified Information*, 2006, http://www.state.gov/m/ds/clearances/60321.htm

Personnel Management (OPM);[8] however, additional methods of investigation may create a more complete "whole-person" understanding of a security clearance candidate. The character traits may help identify ways modern technology can be leveraged to help determine whether a current security or potential security clearance holder be an unacceptable risk based on questionable behavior or specific characteristics.

The research relies on published, open-source literature and provides answers to who, what, where, why, and when regarding disclosed classified information to determine common character flaws demonstrated by those who have violated the trustworthiness represented by having been granted a security clearance. This research effort contains detailed research of known perpetrators, categorization of specific character traits, analysis of those categories, and conclusions based on that analysis. The cases studied are: Aldrich Ames, Ana Belen Montes, Chelsea Manning, Brian Regan, Bryan Underwood, Greg William Bergersen, Hassan Abu-Jihaad (Paul R. Hall), Robert Hanssen, John Walker, Jonathon Pollard, and Edward Snowden. Selection is based on unauthorized disclosure since the 1980s, including 1985—referred to as the "year of the spy."

The research resulted in findings and includes detailed open-source readings, gleaning characteristics of subjects from the readings, and an analysis of these characteristics to determine which are common among the subjects studied. Research outline:

- Read any available open-source readings
- Record details of commonality between cases
- Analyze most common behavioral characteristics
- Determine if additional observable behavioral characteristics exist
- Provide recommendations
    - Role of technology
    - Insider threat training/awareness

[8] Initial adjudication standards were established under Executive Order 10450, *Security Requirements for Government Employment*, dated April 27, 1953. The adjudicative guidelines were last updated in December 2005 and have been under revision by the Office of the Director of National Intelligence since 2009.

- Utilization of “see something, say something” campaign

D. OVERVIEW OF UPCOMING CHAPTERS

The chapters are laid out as follows:

- Chapter II provides the literature review conducted for this research.
- Chapter III provides the history of information classification policy.
- Chapter IV provides the background of unauthorized disclosure and the “insider threat.”
- Chapter V provides the security clearance process including the 13 adjudicative guidelines.
- Chapter VI discusses the role of technology in the security clearance process today.
- Chapter VII provides the biographical sketches of known cases reviewed.
- Chapter VIII provides a discussion of the gathered data and analysis of the most and least common identifiable personality characteristics of known offenders.
- Chapter IX provides recommendations, including limitations to eliminating unauthorized disclosure, implementation issues, and opportunity for future research.

THIS PAGE INTENTIONALLY LEFT BLANK

II. LITERATURE REVIEW

Recent unauthorized disclosures of classified information by Chelsea Manning and Edward Snowden, along with the tragic shooting event at the Navy Yard in Washington, District of Columbia (DC) involving Aaron Alexis, have raised questions regarding the current policies and procedures of granting and retaining a United States government security clearance. On October 31, 2013, the Senate held a hearing regarding the Navy Yard shooting and security clearances. During that hearing, Senator Tom Carper, the Homeland Security and Government Affairs Committee Chairman, stated he believes the following questions must be answered to improve the system:

1. Are the right risk factors identified and looked at in attempting to identify people who should or should not be trusted with our nation's secrets,
2. What important information is being missed in background investigations which rely heavily on self-reporting, and
3. What should trigger a reinvestigation?[9]
4. What effect has sequestration had on the security clearance process, and
5. What behavior signals an unacceptable risk?[10]

In *Transforming U.S. Intelligence*, Gerber writes:

> The issue of security is a significant one. Security investigators and authorities must do their best to ensure the loyalty and reliability of those applying for and working within the intelligence community. The counterintelligence threat to the United States has not diminished with the collapse of the Soviet Union and the Warsaw Pact. A number of countries and movements, including terrorist organizations, wish to do the United States and its citizens harm. At the least, they want to monitor United States' activities that they perceive as affecting their own national

[9] "Chairman Carper, Ranking Member Coburn Continue Oversight in Wake of Navy Yard Shooting," U.S Senate Committee on Homeland Security and Governmental Affairs, September 19, 2013, http://www.hsgac.senate.gov/media/minority-media/chairman-carper-ranking-member-coburn-continue-oversight-in-wake-of-navy-yard-shooting

[10] "Navy Yard Shooting: Witnesses testified at a Senate Homeland Security and Government Affairs Committee hearing examining the Naval Yard Shooting," C-Span, October 31, 2013, http://c-spanvideo.org/program/YardT

> security. So the granting of a security clearance still involves a great deal of careful work in determining an applicant's suitability and loyalty.[11]

Gerber continues the discussion, noting that applicants may have extensive foreign experience and foreign contacts—and that while this contact may raise suspicions—these personnel may well be the most qualified because of their experiences. Additionally, because of the long lag-time between investigations, hiring, and issuing of clearances, some of the best-qualified candidates may give up on waiting to fill a given position. This theory may not be relevant in today's economy, in which jobs are not only difficult to obtain, but the value of obtaining a clearance can increase a candidate's marketability. Much like gang members joining the armed forces to learn military training, one must wonder what percentage of employees seek a position that requires a clearance only for the purpose of obtaining access to classified information.

This literature review focuses primarily on personnel who held clearances and committed espionage/unauthorized disclosure to determine if there are measures the government can take to hold employees granted a security clearance more accountable. Secondly, it looks broadly at the history of the security classification policy and how the system currently works.

A. LEGAL FRAMEWORK

Several executive orders and intelligence community directives established the security classification program. Executive Order (E.O.) 10450 establishes the foundation of the security clearance process, calling for conditions of reliability, trustworthiness, good conduct and character, and loyalty to the U.S. The order calls for consistent standards of investigation and adjudication across all agencies and specifies what must be included in the investigation, including a national agency check and written inquiries (Section 3.a). It further lists the requirements for investigation: (Section 8.a)[12] and establishes the initial adjudication standards.

---

11 Jennifer E. Sims, and Burton Gerber, eds., *Transforming U.S. Intelligence* (Washington, DC: Georgetown University Press, 2005), 186.

12 Exec. Order No. 10450, 18 Fed. Reg. 2489 (Apr. 27, 1953), 936.

E.O. 12968 "establishes a uniform federal personnel security program [under the Office of Personnel Management] for employees who will be considered for initial or continued access to classified information"[13] and the first uniform adjudicative guidelines. Section 1.2 discusses who may or may not be granted access to classified information and stipulates the three requirements that must be fulfilled prior to an employee being granted access (determined eligible, have a need-to-know, and having signed Standard Form (SF) 312, Classified Information Nondisclosure Agreement).[14] Section 1.3 discusses the required financial disclosure of an applicant.[15] Part 2 of the order discusses determinations of eligibility including reciprocity between agencies,[16] and Part 3 discusses standards of eligibility including reinvestigation requirements.[17] Additionally, Section 6.2 discusses employee responsibilities, including "protect[ing] classified information…from unauthorized disclosure [and] report[ing] contact with…foreign nationals…." Finally, Section 6.4 advises of sanctions against those who disclose classified information.[18]

Executive Order 13381 directs agencies to be "uniform, centralized, efficient, effective, timely and reciprocal." Under this order, the director of the Office of Management and Budget (OMB) is named responsible for effective implementation of the policy.[19]

Executive Order 13467 amends E.O. 12968, by inserting Section 3 (requiring continuous evaluation for clearance holders (as directed in Section 3.b.(i)); Section 2 (stresses reciprocity of investigations and adjudications by all agencies); Section 2.2 (establishes the Performance Accountability Council and its responsibilities); and Section 2.3 (establishes the roles of suitability executive agent, under the Office of Personnel

13 Exec. Order No. 12968, 60 Fed. Reg. (Aug. 4, 1995), 40245–40254.

14 Ibid.

15 Ibid.

16 Ibid.

17 Ibid.

18 Ibid.

19 Exec. Order No. 13381, 70 Fed. Reg. 37953 (Jun. 30, 2005), 37953–37955.

Management (OPM) and security executive agent, under the Office of the Director of National Intelligence (ODNI). The order also establishes the Suitability and Security Clearance Performance Accountability Council.[20] Continuous evaluation (CE) is defined as:

> reviewing the background of an individual who has been determined to be eligible for access to classified information (including additional or new checks of commercial databases, Government databases, and other information lawfully available to security officials) at any time during the period of eligibility to determine whether that individual continues to meet the requirements for eligibility for access to classified information.[21]

A 2005 memorandum to the assistant to the president for National Security Affairs (NSA) delineates the process and guidelines personnel security clearance adjudicators must use in order to make clearance determinations for applicants.[22] Naturally, the adjudication process will always involve a certain amount of personal bias and interpretation and is susceptible to human error or intentional misinterpretation since it is unlikely technology only would be relied upon for the adjudicative process.

Intelligence Community Directive (ICD) *700* mandates an integration of counterintelligence and security functions for the purpose of protecting national intelligence and sensitive information and, among other things, to strengthen:

> deterrence, detection, and mitigation of insider threats, defined as personnel who use their authorized access to do harm to the security of the U.S. through espionage, terrorism, unauthorized disclosure of information, or through the loss or degradation of resources or capabilities.[23]

---

[20] Exec. Order No. 13467, 73 Fed. Reg. 128 (Jun. 30, 2008), 38103–38108.

[21] Ibid.

[22] Stephen J. Hadley to William Leonard, *Adjudicative Guidelines for Determining Eligibility for Access to Classified Information* [memorandum], December 29, 2005, http://fas.org/sgp/isoo/guidelines.html

[23] Office of the Director of National Intelligence, *Intelligence Community Directive Number 700: Protection of National Intelligence* (Washington, DC: Office of the Director of National Intelligence, 2012), § D.4.d.

Under *Intelligence Community Directive* (ICD) *701*,[24] senior officials of the Intelligence Community (IC) must immediately notify the director of National Intelligence (DNI) and, if applicable, "law enforcement of any actual or suspected unauthorized disclosure of classified information, including any media leak, that is likely to cause damage to national security interests, unless the disclosure is the subject of a counterespionage or counterintelligence investigation."[25]

Intelligence Community Directive (ICD) *704* establishes policy for sensitive compartmented information (SCI) and its protection and provides for the ODNI oversight of the program. Section D.4 allows for temporary access during national emergencies. Section E lists standards required to be eligible to receive a clearance while Section F lists exceptions to those standards.[26]

Executive Order 13526, Classified National Security Information, provides "a uniform system for classifying, safeguarding, and declassifying national security information..." and stresses that "protecting information critical to our Nation's security and demonstrating our commitment to open Government through accurate and accountable application of classification standards and routine, secure and effective classification are equally important priorities."[27] All information determined to have the potential to cause damage to national security is classified under this order.

Department of Homeland Security (DHS) *Instruction Handbook 121–01-007* provides direction for the DHS Personnel Suitability and Security Program and "establishes the procedures, program responsibilities, minimum standards and reporting

---

[24] Office of the Director of National Intelligence, *Intelligence Community Directive Number 701: Security Policy Directive for Unauthorized Disclosures of Classified Information* (Washington, DC: Office of the Director of National Intelligence, 2007), http://fas.org/irp/dni/icd/icd-701.pdf, 4.

[25] Jennifer K. Elsea, *The Protection of Classified Information: The Legal Framework* (Washington, DC: Congressional Research Service, 2013), 7.

[26] Office of the Director of National Intelligence, *Intelligence Community Directive Number 704: Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information and Other Controlled Access Program Information* (Washington, DC: Director of National Intelligence, 2008), http://www.dni.gov/files/documents/ICD/ICD_704.pdf

[27] Exec. Order No. 13526.

protocols"[28] specifically for DHS and is based upon guidance from ICD 704, E.O. 12968, and E.O. 10450. The DHS instruction has an extensive list of relevant government codes and regulations regarding the personnel suitability and security program. As a policy document, it is useful in understanding how the third largest federal agency runs their personnel suitability and security program and provides insight into DHS's interpretation of the security clearance program, executive orders and intelligence directives.[29]

The Defense Security Service (DSS) has created *Roles and Responsibilities for Personnel Security—A Guide for Supervisors,* which discusses the five elements of the personnel security program (designation of sensitive positions, clearance requirements, investigative requirements, the adjudication process, and continuous evaluation). The concept of a "whole person" is detailed, along with the 13 conditions that may raise concern (adjudicative guidelines) and the nine mitigating factors (general criteria). Self-reporting is stressed,

> Employees who occupy positions of trust or have access to classified information are expected to self-report changes or incidents that may impact their clearances. Once again, the 13 adjudicative guidelines are a valuable tool in determining if a life-event or situation might result in a need to self-report. Self-reporting, while mandatory, is also a question of personal integrity and certainly preferable to the incident or change being discovered.[30]

Additionally, the guide emphasizes the responsibilities of supervisors, especially in the areas of counseling and the Employee Assistance Program.

The Congressional Research Service's (CRS) *The Protection of Classified Information: The Legal Framework* provides a general overview of regulations and laws regarding the protection of classified information using executive orders as frameworks. It includes extensive detail on the current E.O. 13526, including the eight characteristics of information that may cause damage to national security, the three current levels of

---

[28] U.S. Department of Homeland Security, *The Department of Homeland Security Personnel Suitability and Security Program*: *DHS Instruction Handbook 121–01-007* (Washington, DC: U.S. Department of Homeland Security, 2009), 1.

[29] Ibid., 1.

[30] Defense Security Service, *Roles and Responsibilities for Personnel Security: A Guide for Supervisors,* accessed June 2, 2014, http://www.cdse.edu/documents/cdse/Supv_Role_in_PerSec.pdf, 16.

classification (confidential, secret, and top secret), and declassification guidelines. Additionally, it discusses handling procedures of unauthorized disclosures as developed by the Information Security Oversight Office.[31]

B. SECRECY VERSUS TRANSPARENCY

Throughout history, empires, nations, and even commercial businesses protected critical information that, if divulged, could result in the loss of important military, political, financial, and proprietary positions. Although the formality of classifying information is relatively new in the United States, it is conceded by many to be a necessary evil to protect our way of life. At the same time, there are many who feel the government over classifies and the non-transparency classification creates violates our personal freedoms more than it protects our nation. Clearly, classification of information is controversial and can create divisiveness within our society. In protecting national defense, public pressure to declassify information can be as damning as foreign espionage. By the same token, preservation of individual rights and Bill of Rights freedoms may outweigh the need for classification.

In *Secrets and Leaks: The Dilemma of State Secrecy,* Sagar writes regarding the growing debate of unauthorized disclosures, especially in light of the Wikileaks incident. Sagar provides a thorough discussion of the history of U.S. secrecy, beginning with George Washington withholding secrets from Congress, through the Espionage Act of 1917, up to the NSA warrantless wire-tapping program in 2006.[32] He provides compelling pro and con arguments for unauthorized disclosures and notes:

> the emergency of new media, particularly Internet-based communication channels, has…dramatically increased the ease with which reporters, editors and publishers can evade laws or regulations pertaining to the publication of classified information. We live in a world where leaks of classified information can instantly be transmitted to 'information

[31] Elsea, *The Protection of Classified Information*.

[32] Rahul Sagar, *Secrets and Leaks: The Dilemma of State Secrecy* (Princeton, NJ: Princeton University Press, 2013).

> clearinghouses' like WikiLeaks and OpenLeaks and mirrored on websites based around the world.[33]

Sarbin, Carney, and Eoyang discuss historic cases of citizen espionage, noting that incidents of unauthorized disclosure of classified information became more prevalent in the 1980s, in correlation to the increase in security clearances. They assert those who have committed espionage are "self-centered, greedy, irresponsible volunteers…."[34] Sarbin, Carney, and Eoyang remark that the major focus on counterespionage efforts must be on people and that "No profile is uniquely associated with people who are spies. It has not been possible to ascertain a set of characteristics that would fit every spy."[35] They observe espionage is mainly committed for monetary purposes.[36] Sarbin, Carney, and Eoyang also discuss models or frameworks of espionage, including the behavioral chain of espionage (intention, planning/conspiracy, access, acquisition, deception, foreign contact, exchange, consumption, and escape), as well as behavioral countermeasures (e.g., polygraphs, periodic reinvestigations, financial audits, and travel checks).[37]

Fischer explores why espionage happens, remarking that by the 1980s, most spies were volunteers rather than recruited by foreign agents. In addition, she discusses the Defense Personnel and Security Research Center (PERSEREC), including early efforts to categorize all Americans involved with espionage against the U.S. since World War II. Fischer opines that while financial motivation is the most common reason to commit espionage, very few actually received payments. She questions whether espionage is "really a unique type of wrongdoing committed by quite different types of people or is it just one variation of betrayal-of-trust behavior?"[38]

---

[33] Ibid., 178.

[34] Sarbin, Carney, and Eoyang, *Citizen Espionage*, 2.

[35] Ibid., 6

[36] Ibid.

[37] Ibid., 86–89.

[38] Lynn F. Fischer, *Espionage: Why Does It Happen?* (Washington, DC: Department of Defense Security Institute).

C. FINANCIAL CONCERNS IDENTIFIED WITH THE SECURITY CLEARANCE PROGRAM

Several Naval Postgraduate School theses have explored various financial aspects of the cost of obtaining a security clearance. For instance, in 1988 Euske and Ward evaluated whether financial reporting can actually determine the financial health of an individual. They explore two issues: 1) those who receive payments illegally (in cash), and; 2) whether financial issues are an indicator of future unethical behavior. The report notes that prior to 1988, money has been the primary motivator in espionage cases. The findings support what is currently being discussed in Congress—investigations must include publicly accessible records and database searches in background investigations and reinvestigations. The report does not call for review of law enforcement databases, however. Finding opportunities to reduce the overall costs associated with security clearances, while increasing accuracy of data by which a security clearance is granted, would be beneficial under current budget constraints. The thesis discusses "expert systems," which "have the potential to reduce the personnel resources needed, streamline[s] the processing, and eliminate[s] backlogs for financial screening of individuals in positions of trust"[39] and replace initial human evaluations. While expert systems may be less costly than a human workforce, an expert system may not be able to detect potential indicators that would be evident to a human.

In a 2012 thesis, Festa discusses the 13 adjudicative guidelines used during security clearance investigations. The guidelines were last updated in 2005, prior to today's extensive use of social media. The thesis develops "a comprehensive list of current Internet behaviors and used the list to examine Internet behavior in the cases of cleared government employees who have been charged with espionage or terrorism-related crimes since 2008."[40] The thesis explores the idea of cyber-vetting, which, based on recent events, may give useful insight into a clearance holder's personality. For

[39] Kenneth J. Euske, and Deborah P. Ward, "The Use of Financial Information in Security Clearance Procedures" (master's thesis, Naval Postgraduate School, 1988), 9.

[40] James. P. Festa, "New Technologies and Emerging Threats: Personnel Security Adjudicative Guidelines in the Age of Social Networking" (master's thesis, Naval Postgraduate School, 2012), http://hdl.handle.net/10945/27829, v.

example, reviewing an employee's or potential employee's Facebook page could provide substantial information of personal beliefs or help predict future actions.[41] Four key questions were explored by examining recent espionage cases:

1. What online activities are insider threats engaging in?
2. How has online activity changed over time?
3. How can new technology help to mitigate insider threats?
4. Can adjudicative guidelines mitigate the risk?[42]

In 1991, Hill investigated personnel files submitted for top-secret clearances with "derogatory financial information."[43] The debt amount reviewed was $500 in delinquency for at least 120 days, which may not be a sufficient debt amount at the time to determine whether a clearance holder is under financial duress. By comparing the Defense Investigative Service's (DIS) "delinquent debt criteria with amount of delinquent debt" and Defense Central Index of Investigation's (DCII)

> final decisions of granting clearances, it was determined that delinquent debt is not significant in determining clearance issuance. The thesis contains an extensive literature review of the security clearance program, number of clearances granted, delays in processing, periodic reinvestigations, adjudication processes, financial motives to commit espionage and supervisory oversight.[44]

While financial motives do need to be explored, a broader perspective must be considered in order to get an overall picture of problems with the clearance process. The sample size used for Hill's study was not sufficient when compared with the total number of new investigations undertaken. Hill did not study other indicators of unsuitability, such as behavioral or criminal issues. His findings recommend raising the study threshold to $1000, although that would most likely still be inadequate.[45]

---

[41] For example, see the article on a former Transportation Security Agency employee who maintained a racist, homophobic website at http://splcenter.org/blog/2013/08/26/war-is-on-writes-dhs-employee-who-operates-racist-homophobic-website-calling-for-killing-of-whites/

[42] Festa, "New Technologies and Emerging Threats," 3.

[43] Henry J. Hill, "Impact of Altering the Delinquent Debt Threshold Used for Background Investigation Expansion on the Denial Rate of Security Clearances" (master's thesis, Naval Postgraduate School, 1991), iii.

[44] Ibid., iii.

[45] Ibid.

D. EXAMPLES OF UNAUTHORIZED DISCLOSURE BY SECURITY CLEARANCE HOLDERS

Daniel Ellsberg's disclosures in the "Pentagon Papers" are perhaps one of the earliest and best-known modern disclosures of classified information. While formally charged under the Espionage Act of 1917 for releasing classified information, Ellsberg was never convicted of espionage. The case was dismissed for gross governmental misconduct and illegal evidence gathering. Though perhaps his accounts are one-sided, Ellsberg has published extensively. In *Secrets: A Memoir of Vietnam and the Pentagon Papers*, Ellsberg discusses his career from his beginning in the United States Marine Corps (USMC), to becoming a Pentagon official, to his release of 7000 pages of top secret information regarding the conflict in Vietnam through four presidential administrations.[46] In *Papers on the War*, Ellsberg dissects via essays what he considers the most damaging pages of the Pentagon Papers.[47] This book could assist those with insight as to why subsequent disclosures have occurred and what goes through the minds of those who disclose classified information.

Several congressional hearings and subsequent investigations regarding the Pentagon Papers occurred. For example, *Inquiry into the Alleged Involvement of the Central Intelligence Agency in the Watergate and Ellsberg Matters*[48] and *Watergate Reorganization and Reform Act of 1975: Hearings before the Committee on Government Operations*[49] were overseen. In 1984, Hougan discusses the events of the Watergate scandal utilizing formerly classified documents from the Federal Bureau of Investigation (FBI) and the Central Intelligence Agency (CIA) and recorded interviews. He concludes

---

[46] Daniel Ellsberg, *Secrets: A Memoir of Vietnam and the Pentagon Papers* (New York: Viking Press, 2002).

[47] Daniel Ellsberg, *Papers on the War* (New York: Simon and Schuster, 1972).

[48] *Inquiry into the Alleged Involvement of the Central Intelligence Agency in the Watergate and Ellsberg Matters, House Committee on Armed Services, Special Subcommittee on Intelligence*, 94th Cong. (1975), http://babel.hathitrust.org/cgi/pt?id=uc1.b4351138#view=1up;seq=9

[49] *Watergate Reorganization and Reform Act of 1975: Hearings before the Committee on Government Operations, Senate Committee on Government Operations*, 94th Cong. (1975), http://www.fordlibrarymuseum.gov/library/document/0204/1512004.pdf

the CIA was heavily involved with the team that broke into the Watergate hotel and that the director of Central Intelligence played a part in having Nixon removed from office.[50]

Many articles and books have been written on other well-known, former federal employees, such as Aldrich Ames, who committed espionage for the Russians. Grimes and Vertefeuille detail their personal accounts of the identification and pursuit of Ames and provide details of the operational contact Ames had with CIA agents.[51] Another author, Wise, details how Ames was able to spy for such a long period of time and how he was eventually caught.[52] Wise has also written about Robert Hanssen, who is as equally well-known as Ames. In *Spy*, Wise details the motives of Hanssen, as well as his socially degenerate behavior identifiers.[53] Shannon and Blackman, two *Time Magazine* reporters, also portray Hanssen's story—including details from interviews not previously conducted.[54] Cherkashin, the KGB spy who recruited both Ames and Hanssen, has written his own memoirs regarding the "handling" of the men and his own career.[55]

Sulick, the former head of the CIA's clandestine service, details over 40 Americans who have committed espionage against the United States.[56] Sulick describes

> six fundamental elements of espionage, the motivations that drove [these Americans] to spy; access and the secrets that were betrayed; their tradecraft, meaning the techniques of concealing their espionage; their exposure; their punishment; and, finally, the damage they inflicted on America's national security.[57]

---

[50] Jim Hougan, *Secret Agenda: Watergate, Deep Throat and the CIA* (New York: Random House, 1984).

[51] Sandra Grimes, and Jeanne Vertefeuille, *Circle of Treason: A CIA Account of Traitor Aldrich Ames and the Men He Betrayed* (Annapolis, MD: Naval Institute Press, 2012).

[52] David Wise, *Nightmover: How Aldrich Ames Sold the CIA to the KGB for $4.6 Million* (New York: Harper Collins Publishers, 1995).

[53] David Wise, *Spy: The Inside Story of How the FBI's Robert Hanssen Betrayed America* (New York: Random House Trade Paperbacks, 2003).

[54] Elaine Shannon, and Ann Blackman, *The Spy Next Door: The Extraordinary Secret Life of Robert Phillip Hanssen, the Most Damaging FBI Agent in U.S. History* (Boston: Little Brown. Boston, 2002).

[55] Victor Cherkashin, and Gregory Feifer, *Spy Handler: Memoir of a KGB Officer: The True Story of the Man Who Recruited Robert Hanssen and Aldrich Ames* (Cambridge: Basic Books, 2005).

[56] Michael J. Sulick, *American Spies: Espionage against the United States from the Cold War to the Present* (Washington, DC: Georgetown University Press, 2013).

[57] Ibid., 7.

Sulick also looks at the history of spying in America beginning with the Civil War through the Cold War.[58]

Many well-recognized newspapers have published extensively on Edward Snowden's disclosures of classified information and the effect that such disclosures have had on the intelligence community and relations between the United States and many western countries. Articles include discussions about whether his disclosures should be considered an act of "whistleblowing" or "treason,"[59] the division of citizens' opinions regarding him,[60] possible harm done to foreign relations regarding his disclosures,'[61] detailed information about what has been released,[62] and congressional responses. Additionally, the papers have thoroughly dissected much of Snowden's career and our current laws have been challenged. The lawyer representing Snowden's father has challenged the PATRIOT Act,[63] and Senator Dianne Feinstein welcomes a Supreme Court review as to whether NSA bulk surveillance is legal.[64] While newspaper accounts are not necessarily academic, they give an excellent glimpse into the thoughts of the American people (via personal interviews) and the political climate overall. Often "intelligence data" is first reported by news outlets—although this is probably also a result of an "independent source." For example, in Luke Harding's account of Snowden, he finds Snowden's motives remarkable in that he believes Snowden truly wanted to expose the National Security Agency's unwarranted practices and wanted nothing in

---

58 Michael J. Sulick, *Spying in America. Espionage from the Revolutionary War to the Dawn of the Cold War* (Washington, DC: Georgetown University Press, 2012).

59 Aaron Blake, "Americans: Snowden is a Whistleblower, not a Traitor. Numerous Members of Congress have Labeled Edward Snowden a Traitor, but the American People Aren't on-board Yet," *Washington Post*, July 12, 2013.

60 Peter Swire, "The Culture War over Snowden," *Washington Post*, January 30, 2014.

61 Kathleen Hennessey, "Brazilian President Snubs U.S.; The Key Ally, Angry over Spying Exposed by Edward Snowden, Calls off a State Visit to Washington," *Los Angeles Times*, September 18, 2013.

62 Peter Grier, "Edward Snowden Leaks again: Five Takeaways from the 'Black Budget,'" *The Christian Science Monitor*, August 29, 2013.

63 T. R. Goldman, "In the Snowden Case, Bruce Fein Finds the Apex of a Long Washington Legal Career," *Washington Post*, August 12, 2013, http://www.washingtonpost.com/lifestyle/style/in-the-snowden-case-bruce-fein-finds-the-apex-of-a-long-washington-legal-career/2013/08/11/82ad187a-011b-11e3-9a3e-916de805f65d_story.html

64 Ken Dilanian, "A Post-Snowden Spying Climate; The NSA Contractor's Leaks Mark a Turning Point in U.S. Intelligence, Experts Say," *Los Angeles Times*, December 22, 2013.

return.[65] Likewise, Glen Greenwald depicts Snowden as a hero for courageously informing the public about government secrecy. He observes,

> Often, whistle-blowers like Snowden are demonized as loners or losers, acting not out of conscience but alienation and frustration at a failed life. Snowden was the opposite; he had a life filled with the things people view as most valuable. His decision to leak the documents meant giving up a long-term girlfriend who he loved, a life in the paradise of Hawaii, a supportive family, a stable career, a lucrative paycheck, a life ahead full of possibilities of every type.[66]

On the other hand, General Mike Hayden believes Snowden is "a troubled young man—morally arrogant to a tremendous degree—but a troubled young man."[67] Hayden went on to predict Snowden would end up like other defectors to Russia: "Isolated, bored, lonely, depressed—and most of them ended up alcoholics."[68]

E. SECURITY CLEARANCE PROGRAM CONCERNS

While not an issue of unauthorized disclosure, the Navy Yard shooting has exposed flaws in the security clearance process that are becoming increasingly evident. Issa, the Chairman of the Committee on Oversight and Reform, calls to attention that the largely automated process of background investigations have sacrificed thoroughness for speed and as a result, it does not catch all pertinent information. Aaron Alexis, despite a history of questionable conduct over several years, was able to secure and maintain a security clearance.[69] Issa recommends that investigators should use the Internet and social media sources to increase the "whole person" investigation, that mental health records should be screened, and that Congress should consider measures to require local

---

[65] Luke Harding, *The Snowden Files: The inside Story of the World's Most Wanted Man* (New York: Vintage Books, 2014).

[66] Glen Greenwald, *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State* (New York: Metropolitan Books, 2014), 47.

[67] Abby Ohlheiser, "That Time Edward Snowden and Gen. Michael Hayden Took a Photo Together—Wearing Smiles and Tuxedos," *Washington Post*, August 13, 2014.

[68] Ibid.

[69] *Slipping Through the Cracks: How the D.C. Navy Yard Shooting Exposes Flaws in the Federal Security Clearance Process, Committee on Oversight and Government Reform*, 113th Cong. (2014) (statement of Darrell Issa, Chairman), http://oversight.house.gov/wp-content/uploads/2014/02/Aaron-Alexis-Report-FINAL.pdf

law enforcement to cooperate with Office of Personnel Management security clearance investigators by providing specific information that is requested on applicants.

In a testimony from the director of the U.S. Government Accountability Office (GAO) to the Subcommittee on Counterterrorism and Intelligence, Farrell, the Director of GAO Defense Capabilities and Management, discusses the various agency roles and responsibilities for the security clearance program. She gives detail regarding the process of obtaining and maintaining a clearance (requirements determination, application, investigation, adjudication, appeals, and periodic reinvestigation). The information most frequently missing from investigative reports are: 1) verification of employment, 2) information on social references, 3) security forms completed properly and 4) no personal subject interview occurs.[70]

In June 2014, U.S. Army Specialist Ivan Lopez opened fire at Fort Hood, killing 3 and wounding 16 before killing himself. The Commanding General of Fort Hood, Lieutenant General Mark Milley, calls for reviewing medical histories for clues regarding unstable psychiatric or psychological conditions. Along with medical histories, the subjects of finance, personal relationships, marital issues, and family health issues should be more thoroughly reviewed.[71] Fort Hood is where Major Nidal Hasan killed 13 and wounded 30 others in 2009. In September 2013, Aaron Alexis went on a similar shooting spree, killing 12. Alexis allegedly suffered from mental issues, claiming to hear low frequency voices in his head, directing him to the shooting.[72]

In 2002, U.S. Attorney General John Ashcroft called for additional measures to reduce unauthorized disclosures of classified information. He places the responsibility for correcting the problem on "all Government officers and employees who are privileged to

---

[70] *Testimony before the Subcommittee on Counterterrorism and Intelligence, Committee on Homeland Security, United States House of Representatives. Personnel Security Clearances: Opportunities Exist to Improve the Quality Throughout the Process*,113th Cong. (2013) (statement of Brenda S. Farrell, Director, Defense Capabilities and Management), http://www.gao.gov/assets/660/658960.pdf

[71] Mathieu Rabechault, "Signs of an Argument before U.S. Base Shooting," *Digital Journal*, April 4, 2014, http://www.digitaljournal.com/news/world/signs-of-argument-before-us-base-shooting/article/379516

[72] Jamal Andress, "Army Specialist Ivan Lopez: What We Know about the Fort Hood Shooter," *ABC*, April 2, 2014, http://www.abc15.com/news/national/army-specialist-ivan-lopez-what-we-know-about-fort-hood-shooter

handle classified Government information."[73] He notes that while technology can assist investigators with identifying and punishing those who commit unauthorized disclosure, technology alone will not substantially reduce those occurrences.

[73] Office of the Attorney General, *Letter to the Honorable J. Dennis Hastert, Speaker of the House of Representatives from John Ashcroft, Office of the Attorney General*, October 15, 2002. http://www.justice.gov/sites/default/files/ag/legacy/2007/07/26/letter_house.pdf

III. HISTORY OF NATIONAL SECURITY INFORMATION CLASSIFICATION

Since the formation of the United States, each president has wrestled with developing information security policy against competing needs for secrecy and transparency. The foundation of open communication originates from the First Amendment of the Constitution, which guarantees freedom of religion, speech, press, public assembly, and petitioning the government for redress of grievances.[74] Yet fluidity within political climates, military operations, and foreign relations has caused government administrations to adjust information security policy to reflect the conditions of the day. The historical perspective provides us a glimpse of how each president perceived the need to protect critical state secrets yet bending to the political climate of his day.

The late nineteenth century saw an increase in the amount of economic and social data that the government collected and circulated. During the first half of the twentieth century, Congress resisted efforts by the executive branch to impose official secrecy on the expanding number of federal agencies.[75] However, as the United States entered World War I, President Wilson signed *The Espionage Act of 1917*, which contains two main provisions: the unlawful procurement of military information and the unlawful disclosure of such information to a foreign government or its agents and criminal penalties that may be imposed as a result.[76]

The onset of World War II increased concern for national security and led to more restrictive information control. Creating the regulated security classification system, a uniform system for classifying, safeguarding and declassifying national security information in the executive branch, President Franklin D. Roosevelt issued Executive Order 8381, Defining Certain Vital Military and Naval Installations and Equipment, in

---

74 U.S. Const., amend. I, http://constitutionus.com/

75 John Shattuck, and Muriel Morrissey Spence, "The Dangers of Information Control," *Technology Review* 91, no. 4 (1988): 64–73.

76 United States Espionage Act, 65th Cong. (1917).

1940. Prior to this, information was designated officially secret only under Department of Army (DA) or Department of Navy (DoN) general orders and regulations. This helped clarify the authority of civilian personnel in classifying national defense information, better protect military information under growing foreign hostilities, and better manage the growing power of the executive branch.[77] Federal civilian employees within the executive branch and the war departments were directed to designate all information pertaining to the military, its facilities, or plans as "restricted," "confidential," or "secret;" however, the terms were not clearly defined in the order.[78]

In 1942, while scientists at the Atomic Research Laboratory at Los Alamos, New Mexico worked on creating the atomic bomb under the Manhattan Project, the Office of War Information issued a government-wide regulation on creating and managing classified materials.[79] Those who worked on the Manhattan Project were required to read and sign either the Espionage Act or a special secrecy agreement, which, if violated, could cause dismissal from employment. Several employees were discovered to have sold or given trade information to the Soviet Union, as indicated when the Soviet Union tested its first atomic weapon, almost an exact replica of "Fat Man."[80]

In 1946, President Harry S. Truman issued *The Atomic Energy Act of 1946*. This act regulated how the federal government would control and manage nuclear technology that had been developed in collaboration with Britain and Canada. It also placed such information in separate categories from other weapons information. The act also established the United States Atomic Energy Commission (AEC), placing nuclear weapon development and nuclear power management under civilian authority. The act introduced the term "restricted data," meaning:

---

77 Harold Relyea, *Security Classified and Controlled Information: History, Status, and Emerging Management Issues* (Washington, DC: Congressional Research Service, 2008), 2.

78 Exec. Order No. 8381, 5 FR 1147 (March 22, 1940), http://www.presidency.ucsb.edu/ws/index.php?pid=75574

79 Anthony Cave Brown, and Charles B. MacDonald, eds., *The Secret History of the Atomic Bomb* (New York: Dial Press, 1977), 201.

80 Daniel Patrick Moynihan, *Secrecy*: *The American Experience* (New Haven, CT: Yale University Press, 1998), 138–139, 144.

> all data concerning the manufacture or utilization of atomic weapons, the production of fissionable material, or the use of fissionable material in the production of power, but shall not include any data which the Commission from time to time determines may be published without adversely affecting the common defense and security.[81]

("Restricted data" and "formerly restricted data" of *The Atomic Energy Act of 1954* differ from national security "restricted" information.) Restricted data was further defined to mean the "design, manufacture or utilization of atomic weapons, the production of special nuclear material, or the use of special nuclear material in the production of energy."[82] The 1954 amendment also introduced the term "formally restricted data," which made atomic energy more accessible to the U.S. military (although the information remained classified). The significant money and time invested in nuclear weapons development, along with their lethality, requires the utmost protection against adversaries obtaining such information. Restricted data and formerly restricted data are innately classified by their very nature as they are nuclear information and have no official declassification date; the information is of the most important held by the government today.

In 1950, President Truman issued Executive Order 10104 preserving policies contained in E.O. 8361, limiting classification authority to the Department of Defense, and adding "top secret" as a fourth category of classification.[83] Increased nuclear testing and the entrance into the Korean War created a more conservative political climate; however, in 1951, President Truman liberalized the rules and agencies for creating and classifying information under the guise of "national security" vice the narrower "national defense" when he issued Executive Order 10290, Prescribing Regulations Establishing Minimum Handling Standards for the Classification, Transmission, and Handling, by Departments and Agencies of the Executive Branch, of Official Information Which Requires Safeguarding in the Interest of the Security of the United States. Additionally, the president, "by virtue of the authority vested in [him] by the Constitution and the

---

[81] Atomic Energy Act of 1946, Pub. L. No. 585 (1946), §10(b) 1.

[82] Atomic Energy Act of 1954, Pub. L. No. 83–703 (1954) Chap. 2, §11(y).

[83] Exec. Order No. 10104, 15 FR 597 (Feb. 1, 1950), http://www.archives.gov/federal-register/codification/executive-order/10104.html, Comp, 298.

statutes, and as the President of the United States,"[84] strengthened the president's position to make official policy and aligned his responsibility to commander-in-chief. Executive Order 10290 was the first executive order to enforce the "use of lowest consistent classification" category consistent with national security to avoid over classification.[85] To avoid confusion with "restricted" information, "restricted data" was specifically removed from E.O 10290 and placed under the Atomic Energy Act of 1946. The executive order also provided instruction on automatic (after a specified event or date) and non-automatic (upon review) downgrading and declassification of information.[86]

In an attempt to limit this range of agencies with classification authority, in 1953, President Dwight D. Eisenhower issued Executive Order 10501, Safeguarding Official Information in the Interests of the Defense of the United States, which reinstated "national defense" as the standard for creating classified information. Additionally, classification was limited to three defined levels (top secret, information that unauthorized disclosure could result in exceptionally grave damage to the nation; secret, information that could result in serious damage; and confidential, information that could be prejudicial to the defense interests of the nation). The executive order eliminated the "restricted" category and under it, "the authority to classify defense information or material…shall be limited in the departments and agencies of the executive branch," specifically designated in the order,[87] effectively reduced the number of agencies that could classify data. The order went on to direct the development and maintenance of rigid training and orientation programs.

In 1961, President John Kennedy slightly modified E.O. 10501 with the issuance of Executive Order 10964 which changed automatic declassification four groups: 1, 2, 3, and d. Information falling under groups 1 and 2 were excluded from automatic declassification or downgrading. Information under group 3 would be downgraded every

---

[84] Exec. Order No. 10290, 16 Fed. Reg. 188 (Sep. 24, 1951), http://fas.org/irp/offdocs/eo/eo-10290.pdf, 9735–9801.

[85] Ibid., 9795–9801.

[86] Ibid.

[87] Exec. Order No. 10501, 18 FR 7049 (November 5, 1953), http://fas.org/irp/offdocs/eo10501.htm

12 years until the lowest classification level was reached but not automatically declassified. Information under group d would be downgraded at three year intervals until the lowest classification level was reached and automatically declassified 12 years after the date of issuance.[88]

In 1972, President Richard M. Nixon issued Executive Order 11652, Classification and Declassification of National Security Information and Material, narrowing the classification system. The executive order reduced the number of agencies authorized to classify data, established a general declassification schedule limiting the duration information may remain classified, established mandatory review provisions to address requests to review current classification levels of information, recognized specific information prohibited from being classified, and stipulated that information must be marked to indicate which portions are classified.[89] While the E.O may have helped decrease the amount of classified material being produced, as well as establish a timeline for document declassification, "The Pentagon Papers" scandal negated much of the intended openness of the order. Daniel Ellsberg disclosed top secret Pentagon papers detailing the history of U.S. involvement in Southeast Asia to *The New York Times*, it published the documents under First Amendment rights.[90]

The Nixon administration, in office at the time of the disclosure, made strong allegations that the publication of these documents could seriously harm national security. This led to the first attempt in American history for the federal government to restrain the publication of a newspaper in the name of national security. Ellsberg was charged with conspiracy, espionage, and theft of government property. All charges against him were eventually dismissed under the right to free press.[91] The disclosure of the Pentagon papers and the subsequent actions by the federal government created an

---

88 Exec. Order No. 10964, 26 FR 8932 (September 20, 1961), §1.b (a) (b) (c), and (d), http://fas.org/irp/offdocs/EO10964.htm

89 Exec. Order No. 11652, 37 CFR 520 (March 8, 1972), http://fas.org/irp/offdocs/eo/eo-11652.htm, 9.

90 Raymond. W. Apple, Jr., "25 Years Later. Lessons Learned from the Pentagon Papers," *The New York Times*, June 23, 1996, http://www.nytimes.com/1996/06/23/weekinreview/25-years-later-lessons-from-the-pentagon-papers.html

91 "Judge William Byrne: Ended Trial over Pentagon Papers," *Washington Post*, January 15, 2006, http://www.washingtonpost.com/wp-dyn/content/article/2006/01/14/AR2006011401165.html

environment in which the press and the public became more distrustful of the government and questioned its openness. The debate remains whether the disclosure of the Pentagon papers did in fact damage national security. The dismissal of the charges against Ellsberg have had a lingering effect on the "credibility gap" between the public and the government, as well as transparency policies of subsequent administrations. Senator Birch Bayh supported the publication of the Pentagon papers stating:

> The existence of these documents, and the fact that they [the administration] said one thing and the people were led to believe something else, is a reason we have a credibility gap today, the reason people don't believe the government. This is the same thing that's been going on over the last two-and-a-half years of this administration. There is a difference between what the President says and what the government actually does, and I have confidence that they are going to make the right decision, if they have all the facts.[92]

In 1978, President Jimmy Carter issued Executive Order 12065, National Security Information, which continued to relax classification requirements. "In order to balance the public's interest in access to Government information with the need to protect certain national security information from disclosure," E.O. 12065 identified seven categories of classifiable information:

a) military plans, weapons or operations;

b) foreign government information;

c) intelligence activities, sources, or methods; foreign relations or foreign activities of the United States;

d) scientific, technological, or economic matters relating to national security;

e) United States government programs for safeguarding nuclear materials or facilities; or

f) other categories of information which are related to national security and which require protection against unauthorized disclosure as determined by the President, by a person designated by the President…, or by an agency head.[93]

---

92 "The Pentagon Papers," *UPIbeta Archive Radio*, 1971, http://www.upi.com/Archives/Audio/Events-of-1971/The-Pentagon-Papers/

93 Exec. Order No. 12065, 43 FR 28949 (June 28, 1978), §1-301, http://fas.org/irp/offdocs/eo/eo-12065.htm

E.O. 12065 continued automatic declassification, enacted a policy of using a less restrictive classification designation when there is reasonable doubt as to the classification existed, changed the "confidential" definition to require "identifiable damage" rather than simply damage, and established the Information Security Oversight Office (ISOO) to ensure compliance with the order. A more conservative approach to classification was adopted in 1982 by President Ronald Reagan. He issued Executive Order 12356, National Security Information, which expanded the levels of classified information to:

1) the vulnerabilities or capabilities of systems, installations, projects, or plans relating to national security;

2) cryptology; [or]

3) a confidential source….[94]

Classifiers were instructed to err on the side of *classification*;[95] and automatic declassification requirements (after a certain time period or event) were removed. Furthermore, E.O. 12356 removed the requirement for the classifier to describe "identifiable damage," and the executive order allowed for reclassification of national security information if the declassified information required protection in the interest of national security and could be reasonably recovered.[96] Regarding E.O. 12356, Steven Garfinkel, the Director of the General Services Administration's Information Security Oversight Office, states, "… our oversight experience shows that over the past decade the number of decisions to classify information is relatively constant. The most important variable is not the particular information security system in place, but rather the status of world affairs."[97] Around the time the executive order went into effect, the U.S. and North Atlantic Treaty Organization (NATO) allies and the Soviet Union were embroiled in the Cold War and stockpiles of nuclear weapons in both countries had swelled. President

---

94 Exec. Order No. 12356, 47 FR 14874 and 15557 (April 2, 1982) §1.3.(a), http://www.archives.gov/federal-register/codification/executive-order/12356.html

95 Ibid.

96 Ibid.

97 Gerald A. Schroeder, "An Overview of Executive Order 12356," *FOIA Update* 3, no. 3 (1982), http://www.justice.gov/oip/blog/foia-update-guest-article-overview-executive-order-12356

Reagan's expanded classification policy granted federal officials increased authority to classify more information than had been previously classified.

In 1995, President Bill Clinton adopted a less restrictive classification policy under Executive Order 12958, Classified National Security Information. During this time, several eastern European countries were taking on a democratic government, and the Cold War concluded following the collapse of the Soviet Union. Classification categories were reduced from 10 to seven; cryptology, confidential source and "other categories of information which are related to national security" were removed from classification. The requirement to define "identifiable damage" was restored. The main change with E.O. 12958 was in the area of declassification. The previous executive order had no provisions for automatic declassification based upon the time duration from original classification and this executive order directs that if an original classification authority cannot determine an earlier specific date or event for declassification, the information will be marked for declassification, and not exceed, 10 years from the date of the original decision.[98] However, information that concerned any of the seven classification categories and that may retain sensitivity could be extended an additional 10 years. Along with imposed deadlines for declassification of classified information, E.O. 12958 made information more difficult to classify.

In 2003, following the events of September 11, 2001 and the launching of the global war on terror (GWOT) military campaign, President George Bush issued E.O. 13292, adding two classification categories: "vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security, which includes defense against transnational terrorism" and "weapons of mass destruction." This again increased the amount of information to be classified. The order also eased the reclassification of declassified records, postponed automatic declassification, eliminated the requirement for agencies to prepare declassification records, and authorized the director of central intelligence (DCI) to object to declassification of information determined eligible by the Interagency Security

[98] Exec. Order No. 12958, FR 76 (April 17, 1995), §1.6(c); 1.6(d), 60, http://www.gpo.gov/fdsys/pkg/FR-1995-04-20/pdf/95-9941.pdf, 19825–19843.

Classification Appeals Panel (ISCAP), which would remain protected, unless the president reversed the decision.[99] Automatic declassification of records classified over 25 years had been postponed for over three years, thus E.O. 13292 provided for more information to be classified and for longer periods of time.

Finally, in 2009, President Barack Obama issued E.O. 13526, Classifying National Security Information, rescinding previous orders. In order to improve openness of the government to the public, President Obama ordered two studies into the amount of information the executive branch was classifying. Additionally, protecting "controlled unclassified information" and "sensitive but unclassified" information policy was to be reviewed and standardized across all agencies.[100] The order directed creation of a National Declassification Center (NDC) to increase declassification efforts across agencies. Moreover, "no information [could] remain classified indefinitely" and deadlines were once again published for declassifying information that was exempted from within 25 years.[101] The three levels of classification were carried forward, top secret, in which unauthorized disclosure could reasonably be expected to cause exceptionally grave damage to national security; secret, which could be expected to cause serious damage; and confidential, which could reasonably be expected to cause damage.

E.O. 13526 declares, "Our democratic principles require that the American people be informed of the activities of their Government. Also, our Nation's progress depends on the free flow of information both within the Government and American people."[102] Over the past 14 years, there has been a significant decrease in spending on declassification and a significant increase in spending on classification management.

In 2012, the federal government spent $9.77 billion dollars on government security classification costs, including $48.65 million on declassification and $1.69

---

99 Exec. Order No. 13292, 68 FR 60 (March 25, 2003), http://www.gpo.gov/fdsys/pkg/FR-2003-03-28/pdf/03-7736.pdf, 15315–15334.

100 Exec. Order No. 13556, 75 FR 216 (November 9, 2010), http://www.gpo.gov/fdsys/pkg/FR-2010-11-09/pdf/2010-28360.pdf, 68675–68677.

101 Ibid.

102 Ibid.

billion on classification management.[103] In contrast, in 1998, $199.65 million was allocated for declassification and $212.96 million for classification management.[104] Given the current budget crisis America faces, one could question the efficacy of spending so much money on management of larger and larger quantities of classified documents.

World affairs have helped dictate U.S. administrative policy on protecting classified information. While policy pertaining to classification of sensitive information has been in effect since the 1940s, how well is the U.S. national security information actually being protected? Nowhere in any of the executive orders are there provisions for granting security clearances, who could or could not work with classified documents, or policies anything pertaining to punishment in the case where a classified document was compromised. Can policy be effective to prevent leaks, intentional or unintentional? Examples presented in this thesis show not only policy on information protection may need to be revised, but also security clearance vetting and issuance procedures and implementing a more thorough training program require greater emphasis.

[103] Information Security Oversight Office, *2012 Annual Report to the President* (Washington, DC: Information Security Oversight Office, 2013), http://www.archives.gov/isoo/reports/2012-annual-report.pdf, 26.

[104] Ibid.

IV. DISCUSSION OF INSIDER THREAT AND UNAUTHORIZED DISCLOSURE

State secrecy versus transparency is part of the growing debate regarding unauthorized disclosures, especially in light of recent disclosures by Chelsea Manning and Edward Snowden. Recurring unauthorized disclosures can cause harm by causing damage to intelligence sources and methods, potential loss of life, a financial cost associated with the release as well as harm to international alliances

> because, if repeated often enough, they will lessen the willingness of local sources to share sensitive info with American diplomats (and also make diplomats reluctant to share with each other what they have learned through their careful cultivated networks of informants).[105]

The insider threat "can include damage to the United States through espionage, terrorism, unauthorized disclosure of national security information, or through the loss or degradation of resources or capabilities."[106]

When it comes to those who commit unauthorized disclosure, several terms are bantered about: espionage, whistleblower, spy, patriot, and traitor. Regardless what term is used, it is more important to understand why people choose to spy or disclose sensitive information with which they have been entrusted. In the case of a spy, Sarbin, Carney, and Eoyang list several steps a person takes in becoming a spy. The first step is the opportunity and access to sell or steal classified information and access to a potential customer. They describe the remaining steps:

> Second, the prospect of espionage must occur to the potential spy and not be dismissed out of hand; the behavior must be 'available' or conceivable. Perhaps in some cases the opportunity comes along first and then the possibility comes to mind; in others, the idea arises, and then the opportunity is sought out. But whatever the order, opportunity and idea are the basic preconditions. Next, the potential spy needs a motive strong enough to take the risk. Fourth, any inhibitions of conscience must be overridden. And last, our potential spy must not be prevented by others, in

105 Sagar, *Secrets and Leaks*, 1.

106 U.S. Department of Defense, *The DOD Insider Threat Program*, Department of Defense Directive Number 5205.16 (Washington, DC: U.S. Department of Defense, 2014), §3.b.

> the form of locked doors, security guards, restrictions on access to classified materials, or other external constraints, from succeeding at espionage. In addition to espionage, this model could describe most types of planned crime.[107]

We know whistleblowers normally try to right a wrong or expose persons in authority applying policy to benefit themselves or friends. Jos, Tompkins, and Hays define whistleblowers as "support[ing]…the idea that universal moral rules exist that ought to guide one's judgments" as determined by a survey of former whistleblowers which 58 percent of the respondents "expressed support for universal moral rules…."[108] Alford argues that whistleblowers are ultimately motivated from "narcissism moralized" and "act out of fear of disassociation with one's ideal self and do not have an empathetic association with the sufferer. Instead, whistleblowers feel morally corrupted by association with an aggressor."[109]

While most people do not admire "tattle-tales," today, whistleblowers have gained a slight measure of respect. Examples of this elevated respect are clearly seen by military veterans whose voices are now being heard because of a handful of U.S. Department of Veterans Affairs (VA) whistleblowers about "wait time" scandals and less than professional care at VA hospitals. One of the more famous whistleblowers was Karen Silkwood, who blew the whistle on unsafe nuclear energy plant production. Protection offered for whistleblowers has improved over the years and was recently strengthened by President Obama when he signed into law *Presidential Policy Directive* (PPD) *19* providing additional protection for intelligence agency employees.[110]

While the concept of "insider threat" has long been recognized (cloaked under the Espionage Act of 1917), the term has come to light recently as a result of unauthorized

---

[107] Sarbin, Carney, and Eoyang, *Citizen Espionage*, 40. (Based on a model by Dr. Howard Timm with the Defense Personnel Security Research Center).

[108] Philip H. Jos, Mark E. Tompkins, and Steven W. Hays, "In Praise of Difficult People: A Portrait of the Committed Whistleblower," *Public Administration Review* 49, no. 6 (November/December 1989): 556.

[109] C. F. Alford, and Corrine Bendersky, "Whistleblowers: Broken Lives and Organization Power," *Labour*, no. 51 (spring 2003): 321–323.

[110] White House, *Protecting Whistleblowers with Access to Classified Information* (Presidential Policy Directive-19) (Washington, DC: White House, 2012), https://www.whitehouse.gov/sites/default/files/image/ppd-19.pdf

disclosures of Manning and Snowden, as well as the tragedy of the Washington, DC Naval Yard shooting carried out by Aaron Alexis.[111] As Sarbin writes,

> Those who sell secrets or collect information for other countries have weakened internal constraints or internal constraints that have failed. These peoples' consciences, their anticipation of feeling guilty or ashamed before others if caught, or their sense of violating an unspoken contract to uphold the well-being of others has not overcome the opportunity, the idea and the motivation to commit espionage. Whatever pricks of conscience they felt, they steeled themselves to ignore them. They told themselves rationalizations and explanations for the behavior they contemplated….[112]

Such as in the case of Julius and Ethel Rosenberg, who were executed for disclosing nuclear information to the Soviet Union, could behavioral characteristics, possibly moral characteristics (or lack thereof) have been observed that would have predicted their unauthorized disclosure?

According to Sarbin, Carney, and Eoyang, "The spy puts himself, his need for money, thrills, or some other satisfaction above the well-being of his fellow citizens and the nation. He is self-seeking, 'doing his own thing,' and 'looking out for number one.'"[113] Unfortunately, these character flaws may not be detected during the personnel security investigative process as noted by the Defense Personal Security Research Center (PERSEREC), especially in new employees or very young employees. Herbig notes, "People change with time while they have access, however, which is why security programs incorporate continuous evaluation measures, and why they update their information on these criteria in order to capture changes of security concern."[114]

Sarbin, Carney, and Eoyang rather succinctly cover the gamut of reasons people turn their back on the government when they opine:

---

[111] In March 2008, despite his failure to disclose the 2004 arrest and several outstanding debts amounting to several thousand dollars, the Navy granted Alexis a secret level clearance. On several occasions in the years leading up to the September 16, 2013 shooting (killing 12 persons), Aaron Alexis could have been stopped—either by a thorough investigation of his background prior to granting him a clearance, continuous evaluation of his competency for a security clearance while he was a naval reservist, or reports of his behavior as a government contractor. *Slipping Through the Cracks*, 20.

[112] Sarbin, Carney, and Eoyang, *Citizen Espionage*, 54–55.

[113] Ibid., 55.

[114] Herbig, *Changes in Espionage by Americans: 1947–2007*, 39.

> Recently detected acts of espionage have been undertaken by self-centered, greedy, irresponsible volunteers. Most of them seem to have been motivated by a desire for money, either out of greed or need. Many of them acted in retaliation for real or imagined wrongs inflicted by someone with authority over them. Personal failures could have stimulated some to defy the law in a mistaken attempt to gain self-esteem.[115]

They continue to say most of the recent crimes are committed by low to mid-level employees, former employees, or military who "became spies out of the desire for revenge, because of disgruntlement with circumstances of their lives, for ideological reasons, for money, at least once for sex, and because of frustration in achieving professional goals"[116] However, Sarbin, Carney, and Eoyang conclude that motivations cannot be matched to a particular personality type.[117]

Established organization practices "such as prioritizing production over security, failure to share information across subunits, inadequate rules or inappropriate waiving of rules, exaggerated faith in group loyalty, and excessive focus on external threats—can be seen in many past failures to protect against insider threats."[118] Employees who report behavioral indicators (e.g., unexplained affluence, foreign trips, unusual working hours) to supervisors may downplay them because of office culture. Supervisors who may observe these behaviors in employees themselves may do the same. In addition, employees may not want to accuse a colleague, overlooking the behavior with regard to the workload or unusual working conditions, nor may they want to admit that an organization may be vulnerable.

Recognition of these behavioral abnormalities or changes has to occur at the lowest level, meaning employee to employee or first-line supervisor level. While agencies may encourage loyalty and employee morale in order to encourage more effective operations:

---

115 Sarbin, Carney, and Eoyang, *Citizen Espionage*, 2.

116 Ibid., 2.

117 Ibid., 6.

118 Matthew Bunn, and Scott D. Sagan, *A Worst Practices Guide to Insider Threats: Lessons from Past Mistakes* (Cambridge: American Academy of Arts and Sciences, 2014), https://www.amacad.org/multimedia/pdfs/publications/researchpapersmonographs/insiderThreats.pdf, 2–3.

> organizational leaders should never assume that their personnel are so loyal that they will never be subject to ideologies, shifting allegiances, or personal incentives that could lead them to become insider threats. Managers should beware of the "halo effect," in which well-liked employees are assumed to be trustworthy (a special case of affect bias, the tendency we all have to assume that something we like for a particular reason has other positive qualities as well).[119]

A successful background investigation does not ensure an employee will not become an insider threat. The Personnel Security Program (PSP) is designed to measure a person's reliability measured against established personnel security criteria (currently there are 13 of those as discussed in Section II.C) and even then is not a good predictor of whether a person is a threat to national security. For example, Manning and Snowden did not fit a template for someone prone to disclose classified information. Both passed successful background checks, and neither had spent years in super sensitive positions. The Intelligence and National Security Alliance (INSA) describe Manning and Snowden as "freedom fighters" rather than threats to national security since those who execute unauthorized disclosures generally did so after an average of 12 years of service. Notwithstanding any length of service, the NSA argues for more stringent background checks.[120] This may reflect the average time it takes for an employee to know a position well enough, have access to materials, achieve the comfort level necessary to steal classified national security information and have the nerve to sell it or disclose it to the general public.

In order to reduce the risk of insider threat, the culture of an organization must be one of loyalty to each other. As put by General Eugene Habiger, the former Department of Energy (DOE) "security czar" and former commander of U.S. strategic forces, "Good security is 20 percent hardware and 80 percent culture."[121] From the smallest team to the entire organization, employees must understand that security is everyone's responsibility.

---

[119] Ibid., 4.

[120] Intelligence and National Security Alliance, Security Policy Reform Council, *Leveraging Emerging Technologies in the Security Clearance Process* (Arlington, VA: Intelligence and National Security Alliance, 2014), http://www.insaonline.org/i/d/a/Resources/LeveragingEmerging_wp.aspx, 4.

[121] Matthew Bunn et al., *Project on Managing the Atom: Advancing Nuclear Security: Evaluating Progress and Setting New Goals* (Cambridge, MA: Harvard Kennedy School, Belfer Center for Science and International Affairs, 2014), 44.

According to Bunn et al., "Establishing clear incentives that make employees understand that they will be rewarded for good security performance is one key element of building such a culture, and of making clear the priority that management places on security."[122]

A second critical aspect of security is employee satisfaction. Bunn et al. explain:

> Disgruntled employees are much more likely to become insiders—and much less likely to proactively help to improve security by reporting odd or suspicious behavior or by creatively looking for security vulnerabilities and ways to fix them. In situations ranging from retail theft to IT [information technology] sabotage, disgruntlement has been found to be a key driver of insider threats.[123]

Thousands of books on management describe methods to reduce employee disgruntlement and create a positive and secure climate in the organization. These include but certainly are not limited to allowing a complaint or suggestion process to address office issues, recognition of and reward for good performance, creation of an environment of fairness, and addressing supervisory failings. As Bunn et al. advocate:

> Efforts to prevent insider threats primarily through screening for loyalty or, conversely, monitoring for ties to malicious terrorist or criminal organizations are insufficient. Such methods will not detect or deter individuals who make poor judgments, even radically poor judgments, in the name of a private interest or even in pursuit of a distorted vision of the public good.[124]

Loyalty to the organization, colleagues, and, ultimately, the American people will aid in employees making sound judgments. It will also decrease the likelihood of unauthorized disclosure.

Chaney explains the psychology of an "insider spy" as

> an intolerable sense of personal failure, as privately defined by that person…. What turns out to be key is how this intolerable sense of personal failure gets managed. Almost always, this is a state of mind based

[122] Ibid., 11–12.

[123] Ibid., 12.

[124] Ibid., 18.

> on male psychology. Over 95% of insider spies are males. Injuries to male pride and ego are at the root of most cases of insider spying.[125]

He goes on to write:

> For a man, maintaining a stable sense of personal worth is key. However, the insider spy experiences three tremendous losses: He suffers two failures before getting caught: His first failure was his inability to successfully navigate his own life; his second failure was discovering that his best attempt to solve his worst life crisis turned out to be a pathetic delusion as he is now merely a puppet on the string of his handler. His third and very public failure is that he could not even succeed at being an insider spy.[126]

Chaney urges that we get away "from mainstream explanations that insider spies are born bad, or that a fixed personality type will predict for insider spying."[127] The usual thoughts of motivations, greed, and ego are less relevant than individual events in a person's life or his or her life stressors (e.g., divorce, death in the family, financial concerns)—the environment in which an individual exists. Because of personal experiences, predicting who may release classified information is not probable.

In September 2014, the Department of Defense (DOD) published *The DOD Insider Threat Program* that

> Establishes policy and assigns responsibilities within DOD to develop and maintain an insider threat program to comply with the requirements and minimum standards to prevent, deter, detect, and mitigate actions by malicious insiders who represent a threat to national security or DOD personnel, facilities, operations, and resources.[128]

Developing insider threat awareness, training, and education will assist in the creation of a cohesive organizational culture—one in which employees know their roles and responsibilities in an agency, regardless of whether or not they hold a security clearance. This culture is critical to protect valuable assets as organizations:

---

[125] David L. Chaney, *Noir: A White Paper*, 2014, http://www.noir4usa.org/wp-content/uploads/2014/07/NOIR-White-Paper-17JUL14.pdf, 2.

[126] Ibid., 7.

[127] Ibid., 2.

[128] Department of Defense, *The DOD Insider Threat Program*, §1.a.

> also have other, often competing, goals: managers are often tempted to instruct employees to bend the security rules to increase productivity, meet a deadline, or avoid inconvenience. And every hour an employee spends following the letter of security procedures is an hour not spent on activities more likely to result in a promotion or a raise. Other motivations—friendships, union solidarity, and familial ties—can also affect adherence to strict security rules.[129]

Directed by the *National Insider Threat Policy*, insider threat programs for the executive branch agencies are "intended to: deter cleared employees from becoming insider threats; detect insiders who pose a risk to classified information; and mitigate the risks through administrative, investigative or other response actions."[130] As such, the *Minimum Standards for Executive Branch Insider Threat Programs* direct employee training and awareness to address:

a. The importance of detecting potential insider threats by cleared employees and reporting suspected activity to insider threat personnel or other designated officials;

b. Methodologies of adversaries to recruit trusted insiders and collect classified information;

c. Indicators of insider threat behavior and procedures to report such behavior; and

d. Counterintelligence and security reporting requirements, as applicable.[131]

The National Counterintelligence and Security Center (NCSC) notes the most damaging United States counterintelligence failures over the past century have been committed by an insider. In each case, the individuals showed behavioral indicators of concern that went undetected "for years due to the unwillingness or inability of colleagues to accept the possibility of treason."[132] Other times, when coworkers reported apprehensions to a supervisor, no action was taken. With early intervention and counseling, individuals at risk for disclosing information may be prevented from doing so. "See something, say something" truly applies for creating an agency culture of

---

[129] Bunn, and Sagan, *A Worst Practices Guide to Insider Threats*, 14.

[130] Office of the Director of National Intelligence, *Minimum Standards for Executive Branch Insider Threat Programs*, http://ncix.gov/nittf/docs/National_Insider_Threat_Policy.pdf, §B.2.

[131] Ibid., §I.1 (a–d).

[132] Office of the Director of National Intelligence, "Insider Threat,"2015, http://www.ncix.gov/issues/ithreat/ 2015.

loyalty—one that may prevent a trusted friend or coworker from disclosing information and spending the rest of his or her life in prison.

The Federal Bureau of Investigation (FBI) has comprised a list of behavioral indicators that may signal an employee at risk:

- Without need or authorization, takes proprietary or other material home via documents, thumb drives, computer disks, or email.
- Inappropriately seeks or obtains proprietary or classified information on subjects not related to their work duties.
- Interest in matters outside the scope of their duties, particularly those of interest to foreign entities or business competitors.
- Unnecessarily copies material, especially if it is proprietary or classified.
- Remotely accesses the computer network while on vacation, sick leave, or at other odd times.
- Disregards company computer policies on installing personal software or hardware, accessing restricted websites, conducting unauthorized searches, or downloading confidential information.
- Works odd hours without authorization; notable enthusiasm for overtime work, weekend work, or unusual schedules when clandestine activities could be more easily conducted.
- Unreported foreign contacts (particularly with foreign government officials or intelligence officials) or unreported overseas travel.
- Short trips to foreign countries for unexplained or strange reasons.
- Unexplained affluence; buys things that they cannot afford on their household income.
- Engages in suspicious personal contacts, such as with competitors, business partners, or other unauthorized individuals.
- Overwhelmed by life crises or career disappointments.
- Shows unusual interest in the personal lives of coworkers; asks inappropriate questions regarding finances or relationships.
- Concern that they are being investigated, leaves traps to detect searches of their work area or home, searches for listening devices or cameras.[133]

[133] Federal Bureau of Investigation. *The Insider Threat: An Introduction to Detecting and Deterring an Insider Spy* [brochure], accessed February 11, 2015, http://www.ncix.gov/issues/ithreat/docs/Insider_Threat_Brochure.pdf

Many people will experience several of these behaviors throughout their lifetimes but are able to cope with stressful situations and will not break the law by unauthorized disclosure of classified information. However, some who lack coping skills will be unable to resist the lure of wrongdoing. A supportive agency culture and employees who are well trained on behavioral indicators will aid in preventing unauthorized disclosures. As such, Sarbin, Carney, and Eoyang urge the development of custodians—those protecting something of value who act:

> in accordance with rules and regulations supplemented by an attitude toward duties, superiors, peers and environment. The custodian's attitude is formed as a result of family relationships, community values, education, professional training, circumstances of employment, fear of retribution for wrongdoing, or anticipation of rewards for proper behavior.[134]

This application must be applied across the board—from the smallest team to the walnut paneled offices of the leaders in the executive branch to prevent unauthorized disclosures.

[134] Sarbin, Carney, and Eoyang, *Citizen Espionage*, 4.

V. THE SECURITY CLEARANCE PROCESS— 13 ADJUDICATIVE GUIDELINES COMPRISING A RANGE OF HUMAN BEHAVIOR USED TO ASSESS TRUSTWORTHINESS

The personnel security clearance process is governed primarily by Executive Order 12968, Executive Order 13467, and the Federal Investigative Standards.[135] Individual agencies may further refine the conditions of obtaining and retaining a security clearance, for example the Department of Defense (DOD) Regulation 5200.2 series or the Department of Homeland Security (DHS) Instruction 121–01-007, *Personnel Suitability and Security Program.* When an executive branch employee (whether military, civilian, or contractor) requires access to classified national security information, that individual must undergo a personnel security investigation (PSI) to determine eligibility to access such information. The investigation and subsequent adjudication process determine loyalty, character, trustworthiness, and reliability of the applicant.[136] According to Defense Security Service (DSS):

> The adjudicative process is the careful weighing of a number of variables known as the "whole person concept." Available, reliable information about the individual, past and present, favorable and unfavorable, is considered in reaching a determination of eligibility. Eligibility for access is granted only where facts and circumstances indicate that access to classified information is consistent with the national security interests of the United States.[137]

First, the agency must identify positions when filled requires the employee access to classified national security information. Once hired, the applicant completes the Standard Form (SF) 86, Questionnaire for National Security Positions, requesting an investigation. The extent of background information supplied by a candidate is dependent on the level of security clearance being requested.

---

[135] Undersecretary of Defense for Intelligence, *Internal Review of the Washington Navy Yard Shooting: A Report to the Secretary of Defense* (Washington, DC: Department of Defense, 2013), 8.

[136] Defense Security Service, *So You Need a Security Clearance: How to Receive and Maintain Your Security Clearance* (Washington, DC: Defense Security Service), http://www.cdse.edu/documents/cdse/Receive_and_Maint_Sct_Clnc.pdf, 2.

[137] Ibid., 2.

- *Top Secret*—information of which unauthorized disclosure could reasonably be expected to cause exceptionally grave damage to the national security.[138] Background information reviews the last 10 years of an applicant's life.

This includes *Sensitive Compartmented Information (SCI)*, which is "classified information concerning, or derived from intelligence sources, methods or analytical process requiring handling within formal access control systems established by the Director of Central Intelligence (DCI)."[139]

- *Secret*—information of which unauthorized disclosure could reasonably be expected to cause serious damage to the national security,[140] or
- *Confidential*—information of which unauthorized disclosure could reasonably be expected to cause exceptional damage to the national security.[141] Background information reviews the last five to seven years for both secret and confidential clearances.

The following background information is reviewed: employment history, education, reference checks, military service record, foreign activities and travel, financial history, police records, and drug and alcohol abuse.[142]

After the background investigation is completed by the Office of Personnel Management (OPM), it is sent to the Central Adjudications Facility (CAF). As defined by the *OPM Suitability Processing Handbook*, adjudication is "An examination of a person's character or conduct over time, resulting in a favorable or unfavorable determination of their employment suitability; eligibility for access to classified information, materials, or areas; or for their retention in Federal employment."[143] An adjudicator at a CAF will

---

138 Exec. Order No. 13526, §1.2(1).

139 U.S. Department of Homeland Security, *Sensitive Compartmented Information Program Management*, Management Directive Number 11043 (Washington, DC: Department of Homeland Security, 2004), §IV.K.

140 Exec. Order No. 13526, §1.2(2).

141 Ibid., §1.2(3).

142 Defense Security Service, *So You Need a Security Clearance*, 7.

143 Kimberley Lew, *Introduction to Personnel Security*, U. S. Department of Headquarters, Office of the Chief Security Officer, http://www.iom.edu/~/media/Files/Activity%20Files/PublicHealth/WorkforceResilience/Kimberly%20Lew.pdf

review all of the information, the "whole person" concept, and assess against the federal adjudicative guidelines to determine eligibility.

- If no significant adverse information is revealed, a security clearance at the level requested by the agency is granted.
- If significant, adverse material develops, a case will be delayed until additional information is gathered and facts are verified. Ultimately, a clearance may be denied.[144]

The four steps of adjudication are (see Figure 1):

- Analyze the background information,
- Apply relevant laws, regulations, and guidelines,
- Request additional information when needed, and
- Communicate the recommendations and decisions regarding [the] clearance.[145]

144 Defense Security Service, *So You Need a Security Clearance*, 7.

145 Lew, *Introduction to Personnel Security Adjudication*, Slide 4.

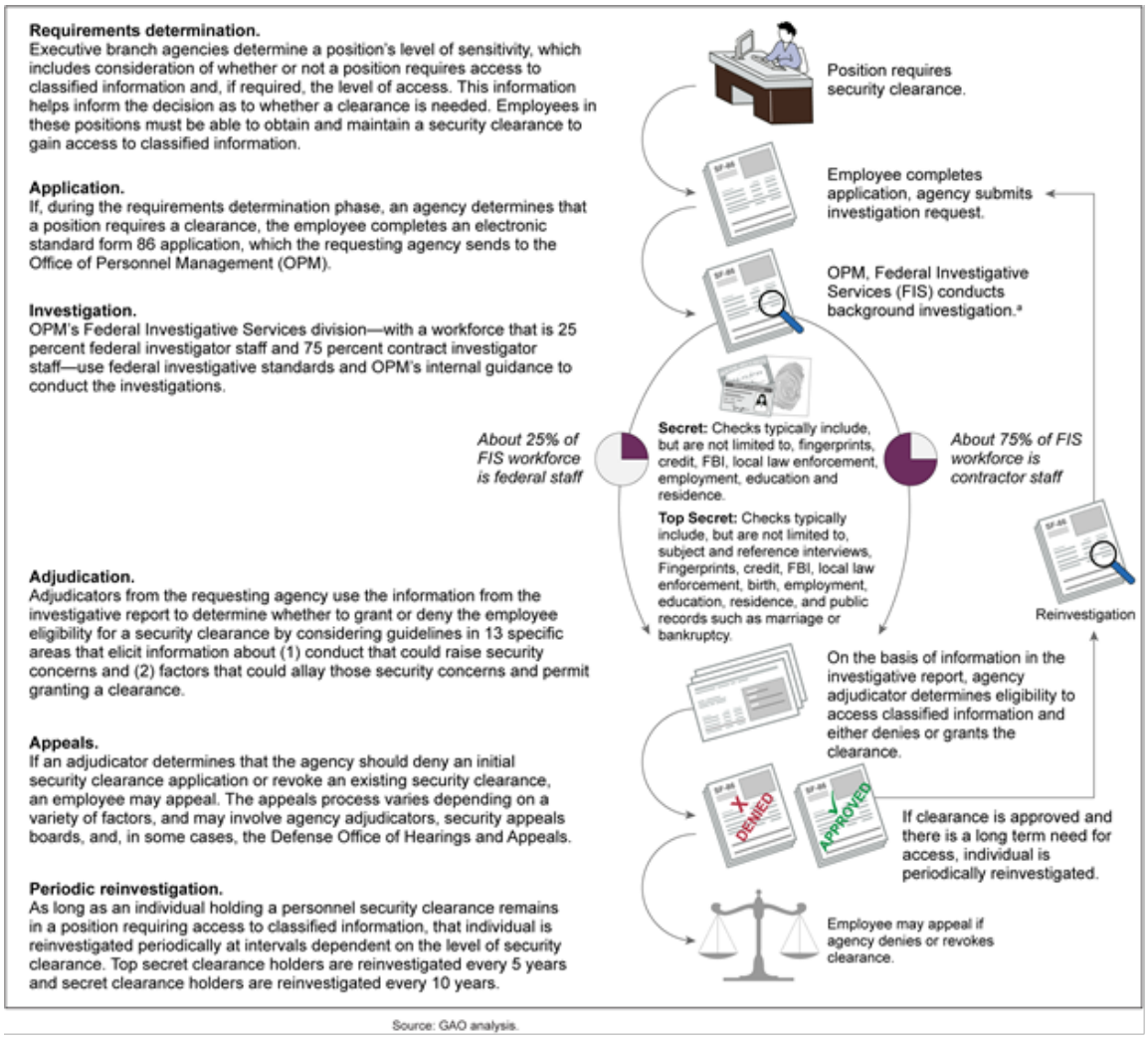

Figure 1. Overview of the Security Clearance Program[146]

The 13 adjudicative guidelines for determining eligibility for access to classified information and eligibility to perform sensitive duties are:

Allegiance to the United States

Actual or threatened use of force or violence in an effort to change government policy, prevent government personnel from performing their assigned duties, or prevent others from exercising their constitutional rights.[147]

146 *Testimony before the Subcommittee on Counterterrorism and Intelligence*, 7.

147 Defense Security Service, *So You Need a Security Clearance*, 13.

Foreign Influence

Unreported personal contacts with personnel from a foreign intelligence service, foreign government, or persons seeking classified, proprietary, or other sensitive information; unreported close and continuing contact with a foreign national, including intimate contacts, shared living quarters, or marriage; or unreported relatives, or unreported contact with relatives, in a foreign country.[148]

Foreign Preference

Exercising benefits of dual citizenship, including possession and use of a foreign passport or other foreign identity documentation without approval.[149]

Sexual Behavior

A pattern of self-destructive or high-risk sexual behavior that the individual is unable to stop or criminal sexual behavior.[150]

Personal Conduct

Recurring pattern of poor judgment, irresponsibility, or emotionally unstable behavior or deliberate omission or falsification of material information about background when applying for security processing.[151]

Financial Considerations

Living or spending beyond one's means including unexplained affluence (unusually large or lavish purchases) or sudden large sums of cash that may indicate illegal source of income or bankruptcy.[152]

Alcohol Consumption

Alcohol-related incidents at work, such as reporting to work or duty in an intoxicated or impaired condition, or drinking on the job or alcohol-related incidents away from work, such as driving while under the influence,

[148] Ibid., 14.

[149] Ibid., 15.

[150] Ibid., 16.

[151] Ibid., 15.

[152] Ibid., 13.

fighting, child or spouse abuse, or other criminal incidents related to alcohol use.[153]

Drug Involvement

Use, possession, or acquisition of illegal/illicit substances or misuse (use other than as prescribed), inappropriate possession, or inappropriate acquisition of prescription medication.[154]

Psychological Conditions

A pattern of significant change from past behavior, especially relating to increased nervousness or anxiety, unexplained depression, hyperactivity, decline in performance or work habits, deterioration of personal hygiene, increased friction in relationships with co-workers, isolating oneself by rejecting any social interaction, or verbal or physical threats toward work associates or family.[155]

Criminal Conduct

Theft, fraud, or a pattern of disregard for rules and regulations (in addition to theft and fraud, this includes taking classified information home at night, or driving while intoxicated).[156]

Handling Protected Information

Collecting or storing classified information outside approved facilities; revealing of classified information to unauthorized persons, including news media; or inappropriate, unusual, or excessive interest in classified information outside one's need-to-know.[157]

Outside Activities

Failure to report paid or volunteer work for any U.S. or foreign media, publisher, academic institution, research organization, or corporation relating to the topics on which one has access to classified information.[158]

---

153 Ibid., 12.

154 Ibid., 13.

155 Ibid., 14.

156 Ibid., 13.

157 Ibid., 16.

158 Ibid., 15.

Use of Information Technology Systems

> Unauthorized entry into any compartmented computer system; storing or processing classified information on any system not explicitly approved for classified processing; or attempting to circumvent or defeat security or auditing systems, without prior authorization from the system administrator, other than as part of a legitimate system testing or security research.[159]

After an employee receives a security clearance, that individual will participate in the Continuous Evaluation Program (CEP or more often simply referred to as CE.) According to the Defense Security Service (DSS), "CEP involves the uninterrupted assessment of a person for retention of a security clearance or continuing assignment to sensitive duties."[160] Continuing evaluation is a critical part of the personnel security process. The clearance holder is subject to periodic reinvestigation (every five years for top secret level clearances, 10 years for secret level, and 15 years for confidential) and

> to a reasonable degree of monitoring by supervisors, co-workers, and security professionals between investigations. These safeguards are necessary because situations and behaviors change over time. Experience shows that individuals approved for a security clearance or position of trust sometimes fall into a pattern of unreliable or untrustworthy behavior after being granted an initial clearance.[161]

Additionally, "the vital need in protect[ing] national security secrets must include rigorous investigation of unauthorized disclosures of classified information to identify the individuals who commit them, and vigorous enforcement of the applicable administrative, civil, and criminal provisions already available."[162]

According to a letter from Office of the Attorney General:

> The responsibility for correcting the problem of unauthorized disclosures of classified information falls squarely upon the shoulders of all Government officers and employees who are privileged to handle classified Government information. Department and agency heads have substantial authority to address the problem of persons who engage in the

159 Ibid.

160 Ibid., 9.

161 Ibid.

162 Office of the Attorney General, *Letter to the Honorable J. Dennis Hastert*, 3.

> unauthorized disclosure of classified information within their own organizations through suspension or revocation of clearances and procedures to terminate employees in the national security interests of the United States.[163]

Personnel entrusted with safeguarding classified material are expected to report potentially significant, factual information that involves themselves or concerns about co-workers that may impact a clearance.[164] Examples of self-reporting requirements by personnel granted security clearances include:

> *Change in Personal Status*—Marital status (marriage, divorce), cohabitation (living in spouse-like relationship, intimate relationship, or becoming engaged), change of name
>
> *Foreign Travel*—A security briefing before any foreign travel, whether for personal or business reasons, clearance for travel to hazardous countries for Sensitive Compartmented Information (SCI)-cleared individuals
>
> *Foreign Contact*—Contact with individuals of any foreign nationality, either within or outside the scope of official duties, in which illegal or unauthorized access to classified or otherwise sensitive information is sought, personal concern of being a target of an attempted exploitation, all close and continuing relationships between SCI-cleared individuals and foreign nations
>
> *Loss or Compromise of Information*—Inadvertent or accidental loss or compromise of classified or other sensitive information because the first priority in such a situation is to regain control of the classified material
>
> *Financial Problems*—Filing for bankruptcy, garnishment of wages, having a lien placed on property for failing to pay a creditor, eviction from a residence for failure to pay rent, or simply the inability to meet all financial obligations
>
> *Arrests*—Any arrest, regardless of whether or not charges were filed, other involvement with the legal system (such as being sued), any circumstance where sworn under oath to testify about association or involvement in questionable activities
>
> *Psychological or Substance Abuse Counseling*—When counseling is needed, seek assistance from employer-sponsored Employee Assistance

---

163 Ibid.

164 Defense Security Service, *So You Need a Security Clearance*, 11.

Program (EAP) or other counseling service. Counseling for certain situations need not be reported if sought the counseling on own employee initiative to help cope. Counseling must be reported if advised to seek counseling because of work performance or other undesirable behavior.[165]

[165] Ibid., 10.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. ROLE OF TECHNOLOGY TODAY

Upon investigating the Washington Navy Yard shooting by Aaron Alexis of September 2003, the Department of Defense (DOD) concluded technology advancements and access to information technology systems and reviewing open-source social media, financial records, and more detailed criminal records would allow for more thorough background investigations of clearance holders.[166] The Office of the National Counterintelligence (ONCI) executive notes:

> Insiders convicted of espionage have, on average, been active for a number of years before being caught. Today more information can be carried out the door on removable media in a matter of minutes than the sum total of what was given to our enemies in hard copy throughout U.S. history. Consequently, the damage caused by malicious insiders will likely continue to increase unless we have effective insider threat detection programs that can proactively identify and mitigate the threats before they fully mature.[167]

These insider threat detection programs rely heavily on improved technology, as well as a cultural change within the intelligence community. Policies and practices will need to be evaluated for effectiveness.

The DOD, the agency that has the most positions requiring security clearances, has been in the forefront of creating new technology. As such, DOD researchers have posed five broad questions regarding analysis of an agency's risk to insider threat:

- Did the organization adequately account for cultural, social, political, legal, economic and other local pressures and stressors in its environment that increased the risk of insider activity across its many potential targets?
- Did the organization lack any important policies or practices (e.g., pre-employment screening, employee monitoring) that could have alerted it to the risks presented by this employee in a more timely way, deterred this individual, managed the risk, or prevented his or her actions?

166 U.S. Department of Defense, *Security from within: Independent Review of the Washington Navy Yard Shooting* (Washington, DC: U.S. Department of Defense, 2013), 4.

167 Office of the Director of National Intelligence, "Insider Threat."

- Did any of the organization's policies and practices have unintentional consequences that made it harder to deter, manage, or prevent insider risks, or did they even increase the risk of insider actions?
- Did the manner in which the organization enforced, or failed to enforce, existing policies and practices contribute to the insider's risk?
- How could modification of the organization's policies and practices have improved the organization's ability to prevent, detect, deter, and manage insider risk?[168]

Most notable in leading alternative screening measures is the DOD Personnel and Security Research Center (PERSEREC), which has spent the better part of two decades developing a program called the Automated Continuous Evaluation System (ACES). As Herbig, Zimmerman, and Chandler explains:

> ACES is an automated computer system that collects data from more than 40 government and commercial electronic records. It uses an applicant's personally identifiable information (PII) obtained from the federal security questionnaire, the Standard Form 86 (SF-86), to check these data sources, verify the information that has been submitted, and leverage the information gathered to collect additional subject information. It applies business rules to analyze the data returned, produces a report that flags issues of potential security concern, and electronically transmits the report to the approved recipient—typically an adjudication facility.[169]

If implemented by DOD, repeated testing by PERSEREC of ACES database mining has shown the security clearance and suitability vetting process can be streamlined while reducing costs. ACES electronic database checks can be used throughout an employee's employment: between an initial background investigation and a periodic reinvestigation, as a tool for elements of the initial investigation or the reinvestigation, as a tool for prescreening military recruits, and as a tool for counterintelligence investigations.[170] By conducting a random review of clearance

---

[168] Eric D. Shaw, Lynn F. Fischer, and Andrée E. Rose, *Insider Risk Evaluation and Audit* (technical report 09–02) (Monterey, CA: Defense Personnel Security Research Center, 2009), http://www.dhra.mil/perserec/reports/pp09-03.pdf, 3.

[169] Katherine L., Herbig, Ray A. Zimmerman, and Callie J. Chandler, *The Evolution of the Automated Continuous Evaluation System (ACES) for Personnel Security* (technical report 13–06) (Monterey, CA: Defense Personnel Security Research Center, 2013), vii.

[170] Ibid., ix.

holders current backgrounds, this technology will assist in determining if personnel are loyal, trustworthy, reliable, and of good character.

In 2013, an ACES

> pilot test with a sample of 3,370 Army service members, civilian employees, and contractor personnel demonstrated that ACES was able to identify 731 individuals with previously unreported derogatory information (21.7 percent of the tested population), prompting 176 reinvestigations to resolve or adjudicate that derogatory information. Of this group, 99 individuals had serious derogatory information (e.g., financial issues, domestic abuse, drug abuse, or prostitution). Based on the results of this test, the Army revoked the clearances of 55 of these individuals and suspended the access of the remaining 44.[171]

Another PERSEREC implementation is the Insider Risk Evaluation and Audit Tool "designed to help the user gauge an organization's relative vulnerability to insider threats."[172] The tool is comprised of

> six categories of internal preventative or mitigating management activities and the selection of evaluation and audit questions in each category is based on the authors' distillation of empirical analysis from a relatively large number of insider cases, academic research, and organizational consultations on insider challenges.[173]

The six functional areas are:

- Policies and Practices
- Recruitment Methods
- Pre-employment Screening
- Effective Training and Education
- Continuing Evaluation and Policy Implementation
- Management Intervention[174]

---

171 Undersecretary of Defense for Intelligence, *Internal Review of the Washington Navy Yard Shooting*, 14.

172 Defense Personnel Security Research Center, *Insider Risk Evaluation and Audit Tool* (PP 09–03), August 2009, http://www.dhra.mil/perserec/reports/pp09-03.pdf, 1.

173 Ibid.

174 Ibid.

A. POLICIES AND PRACTICES

No matter how well written they are, not all policies are applicable to all agencies. Of equal importance is the need for employees, whether they are clearance holders or not, to understand their roles and responsibilities to the government and the American public. Employees must be encouraged and empowered to report suspicious behaviors of their co-workers—or changes in their own lifestyles—without fear of reprisal or lack of subsequent action. According to Shaw, Fischer, and Rose, authors of a 2009 PERSEREC report:

> *Policies and Practices* refers to the rules and guidelines governing employee behavior that have proven critical to deterring, detecting, and correcting potentially harmful behaviors by employees and others. Policies and practices can mandate employee screening, generate both human and IT monitoring and detection systems to enforce regulations, and establish guidelines for investigation and consequences when these risk behaviors are detected. The absence of policies and practices has actually facilitated insider activity and prevented successful prosecutions of significant insider violations. Not only should these guidelines exist, they also must be documented and easily accessible to employees, contractors and subcontractors.[175]

B. RECRUITMENT METHODS

Many agencies encourage employees to refer friends and family to apply for vacant agency positions. PERSEREC case data, however, has determined that often these personal relationships:

> bias the manner in which a hired employee is managed and often lead to at-risk behaviors being ignored, underreported or inadequately sanctioned…. [The] risk of such employees being granted exceptions to policies and practices [is] the detriment of the organization.[176]

Shaw, Fischer, and Rose explain:

> *Recruitment* refers to the manner in which an organization solicits individuals to apply for employment. While some traditional recruitment methods have been extremely useful to organizations, they have also been implicated in some insider incidents as having contributed to an increase

[175] Shaw, Fischer, and Rose, *Insider Risk Evaluation and Audit,* 10.

[176] Defense Personnel Security Research Center, *Insider Risk Evaluation and Audit Tool,* 8.

> in the risk of misconduct. These recruitment practices have included the use of placement groups or "body shops," bounties, recruitment bonuses or employee rewards for referring recruits, and the recruitment and preferential hiring of employee family members or friends. While many of these processes may prove highly valuable in employee recruitment, in some cases they have exacerbated other insider risks when they have resulted in reduced screening or contributed to internal social networks that compete for employee loyalty with the organization.[177]

C. PRE-EMPLOYMENT SCREENING

The report by Shaw, Fischer, and Rose describes:

> *Pre-employment Screening* [as] the manner in which organizations proactively examine potential employees, including contractors, subcontractors and temporary hires, for personal and professional history and characteristics related to their qualifications, fit, and risks as employees. Numerous subjects who committed insider misconduct would probably not have been hired by their organizations if prior activities and personal characteristics—which are the routine target of pre-employment screening measures—had been detected.[178]

Reviewing credit reports and criminal records, contacting personal references, verifying education records, and informal online searches, for example, social media sites, can enhance the "whole person" approach to obtaining a security clearance.

D. TRAINING, EDUCATION, AND PROGRAM EFFECTIVENESS

The report by Shaw, Fischer, and Rose portray the importance of the effectiveness of training and education. They state:

> *Training and Education and Evaluation of Training Effectiveness* (TEE) refers to the way the organization provides formal training and education regarding its policies and practices, especially those directly related to insider risk. TEE also refers to the way in which the organization assesses the effectiveness of education and training efforts through direct evaluation of employee learning and skills, as well as the impact on the risk behaviors targeted in the education and training programs. The frequency with which these TEE programs are updated to take account of

[177] Shaw, Fischer, and Rose, *Insider Risk Evaluation and Audit*, 10.

[178] Ibid., 10.

> feedback on employee learning and risk behavior and to incorporate new information related to insider risks is also examined.[179]

E. CONTINUING EVALUATION AND POLICY IMPLEMENTATION

It is necessary to continue to evaluate employees. As the authors Shaw, Fischer, and Rose describe:

> *Continuing Evaluation and Policy Implementation* refers to the manner in which employees are monitored for continued reliability and personnel security policies are implemented in the work environment. This includes reporting concerns about policy fairness and violations, violation detection, investigation and evaluation, documenting investigative results; determining and administering consequences; and measuring the extent to which policies are put into practice.[180]

F. MANAGEMENT INTERVENTION: ASSESSMENT AND PLANNING

Employee Intervention Assessment and Planning follows from *Continuing Evaluation* and addresses the manner in which managers and their multidisciplinary teams consider possible negative effects of disciplinary or other remedial actions with employees prior to the intervention. Previous research suggests that the routine assessment of an employee's risk of engaging in an insider event prior to serious disciplinary action or other intervention is necessary when he or she has a history of technical violations or problems that were of a security concern. This is especially true prior to the employee's departure from the workplace by involuntary or, in some cases, voluntary termination.[181]

The Intelligence and National Security Alliance (INSA) has recommended combining continuous monitoring and continuous evaluation into a single system Continuous Monitoring and Evaluation (CME). Its 2014 report notes:

> The CME process enables the gathering of external information from hundreds of commercially-approved databases, which is then charted against the baseline SF-86/E-QIP input, other internal agency databases, and checks on the 'clearance health' of the clearance holder. Adjudicators

---

179 Ibid.

180 Ibid., 11.

181 Ibid.

> respond to discrepancies, determining whether to monitor more closely, intervene, or fully investigate flagged issues.[182]

Bringing the trigger event to the proper authority without delay:

> requires an action be recorded and an audit train created….The driver behind the success of CME and ultimately an enhanced PR [Periodic Review] process would be the establishment of an online application and resultant database to replace the paper and online SF-86, SF-85P, and SF-86C. This capability could create a centralized database from which all agencies could access clearance holder information, review changes in real time, see investigative status and 'flags' immediately, and enable portability of clearance eligibility.[183]

As noted in an Intelligence and National Security Alliance report:

> CME adds context for what previously might have been viewed as an isolated event and a single violation of policy. By helping place triggering events in a larger context, it assists in making the best decision possible at the time and provides the audit trail for complete and appropriate accountability.[184]

The U.S. Computer Emergency Readiness Team (CERT) program defines insider threat as:

> a current or former employee, contractor, or business partner who meets the following criteria:
>
> - has or had authorized access to an organization's network, system, or data and
> - has intentionally exceeded or intentionally used that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization's information or information systems.[185]

Silowash et al. note insiders have an advantage over outsiders who want to harm an agency. They explain:

> While mitigation or deterrence measures may be implemented (e.g., firewalls or system access) the insiders are well aware of their

[182] Intelligence and National Security Alliance, *Leveraging Emerging Technologies*, 7.

[183] Ibid., 8.

[184] Ibid., 9.

[185] George Silowash et al., *Common Sense Guide to Mitigating Insider Threats*, 4th ed. (Carnegie Mellon University, Software Engineering Institute, 2012), 4.

> organization's policies, procedures, and technology. In addition, they are often also aware of their vulnerabilities, such as loosely enforced policies and procedures, or exploitable technical flaws in networks or systems.[186]

No matter how effective the technology, agency employees must understand they are responsible for adequately securing classified national security information entrusted to them, including not disclosing the information to others without a need-to-know who may try to gain access to such information via established relationships. Indications of risky employees may also come via social network sites in the form of negative comments. Examples of this would include the Transportation Security Authority (TSA) employee who posted anti-Muslim and anti-gay remarks[187] or the Department of Homeland Security (DHS) employee who maintained an anti-white, anti-gay website.[188] As Shaw, Fischer, and Rose report:

> These activities can pose a threat to national security, endanger the lives or well-being of other employees, or destroy a successful company. Such behaviors include espionage against the United States, theft of intangible assets or intellectual property, sabotage or attacks against networks and information systems, theft or embezzlement, illegal export of critical technologies, and domestic terrorism or collaboration with terrorist groups. While these crimes and offenses may seem dissimilar, the offenders themselves are frequently driven by the same motivations—greed, disgruntlement, conflicting loyalties, ego-satisfaction—and they often exhibit similar early indicators or precursors of subsequent damaging behavior.[189]

As noted by INSA, an online investigation system would improve efficiency and allow for cost savings. Its 2014 report states:

> Investigators no longer need to rely primarily on interviews to find out where a person travels, what they like, who their friends are, what they buy, where they live and what interests they have. Each of us has a 'digital exhaust' or footprint whether we like it or not. Unlike interviews, records

---

186 Ibid.

187 Roy Egan, "Former O'Hare TSA Agent, Fired Over Repeated Anti-Muslim, Racist Facebook Remarks," *Huffington Post*, November 17, 2011, http://www.huffingtonpost.com/2011/11/17/roy-egan-former-ohare-tsa_n_1099331.html

188 Cathy Burke, "Report: DHS Employee Maintains Anti-White, Anti-Gay Site," *Newsmax*, May 21, 2015, http://www.newsmax.com/US/dhs-employee-anti-white/2013/08/22/id/521670/

189 Shaw, Fischer, and Rose, *Insider Risk Evaluation and Audit*, vii.

> can be more easily verified and collectively analyzed for even insignificant changes. This data enables targeted interviews and expands potential interviewees.[190]

Additionally, the report explains:

> a staggering percentage of the population "live" online and do not have that aspect of their lives reviewed as part of the current PR [Periodic Review] clearance policy. No standard exists for a 'neighborhood check' of the "online neighborhood," which is without a fence line and extends beyond national borders and languages. The geographic neighborhood will always remain part of the PR, but information contributing to the 'whole person concept' review occurs online and is being missed.[191]

Also according to the *Leveraging Emerging Technologies in the Security Clearance Process* report, "These same lifestyle changes and technologies actually make establishing a set period for review of five, seven or more years irrelevant and potentially even detrimental to national security."[192]

This becomes more and more evident as we review the cases of insider threats, unauthorized disclosure, and espionage. In the case of Edward Snowden, the unauthorized release of sensitive U.S. government information was dynamic and widespread because of the speed of today's communications. Is the damage any more or any less because America's secrets were electronically broadcast worldwide in a matter of seconds?

---

[190] Intelligence and National Security Alliance, *Leveraging Emerging Technologies*, 4–6.

[191] Ibid., 4.

[192] Ibid.

THIS PAGE INTENTIONALLY LEFT BLANK

VII. BIOGRAPHICAL SKETCHES OF KNOWN OFFENDERS

Open-source research (books, scholarly journals, newspaper articles) were reviewed to determine if there are behavioral characteristics common between the subjects: Aldrich Ames, Ana Belen Montes, Chelsea Manning, Brian Regan, Bryan Underwood, Greg William Bergersen, Hassan Abujihaad (formerly Paul R. Hall), Robert Hanssen, John Walker, Jonathon Pollard, and Edward Snowden. Better known cases had extensive pieces written and provided a wealth of character notes while lesser known persons did not.

A. ALDRICH AMES

A 31-year veteran with the Central Intelligence Agency (CIA), Aldrich Ames was arrested in 1994 for selling classified information to the Russians beginning in 1985. Ames went directly to the Russian embassy in Washington, DC to begin his spying career. He was eventually convicted and sentenced to life in prison.[193] While bank records show Ames was paid $1,538,685,[194] it is estimated he received over $2 million in payment.[195] Among other classified information, Ames disclosed names of Russian agents who had been recruited to spy for the United States. At least 10 of those agents were recalled to Russia and executed..[196]

1. Ego and Intellect

As a child, Ames was encouraged to learn about the finer things in life. After dinner, the family would listen to classical music or jazz while reading individually. By age 10, Ames was reading three or four books each week.[197] When the family relocated

193 Federal Bureau of Investigation, "Famous Cases and Criminals—Aldrich Hazen Ames," accessed May 6, 2014, http://www.fbi.gov/about-us/history/famous-cases/aldrich-hazen-ames

194 Brian Duffy, Edward T. Pound, and Gary Cohen, "The Million Dollar Spy," *U.S. News and World Report*, March 7, 1994, 26.

195 Pete Earley, *Confessions of a Spy: The Real Story of Aldrich Ames* (New York: Berkley Books, 1998), 12.

196 Duffy, Pound, and Cohen, "The Million Dollar Spy," 26.

197 Earley, *Confessions of a Spy*, 21.

to the District of Columbia, Ames' father said, "You have nothing to fear about moving into a new community. You are Ameses. You are special. You are smart and you will do well."[198] This type of encouragement from an early life most likely contributed to Ames' strong ego and extremely high self-esteem. His father despised communism and talked about:

> the life and death struggle taking place between the free and communist worlds… He depicted the suppression of freedom and the brutal conditions of life under communist regimes as being so inhumane and dehumanizing that he said…he would rather see us dead than living under communism.[199]

After Ames accepted his first $50,000 dollars from the Russians for the initial lot of classified information, there was no turning back. According to a book on Ames by Maas,

> They had said they wanted a long-lasting relationship with him. Those were sweet words. There was a comforting, caring quality to them, reflecting the kind of relationship that he had yearned for from his own father and never enjoyed. He was valued![200]

Ames was very successful at being deceptive. During his period of spying, he was able to pass two polygraph exams "which specifically addressed unauthorized contacts and disclosures of foreign nationals…."[201]

2. Addiction

Ames had an addiction to alcohol. When interviewed by Pete Earley, who had access alone with him for over 50 hours, Ames said,

> Drinking has always been a struggle for me. I have vacillated between considering myself beyond self-help and total denial…. For many years…

198 Ibid., 24

199 Ibid., 28.

200 Peter Maas, *Killer Spy: The inside Story of the FBI's Pursuit and Capture of Aldrich Ames, America's Deadliest Spy* (New York: Warner Books, 1995), 58.

201 Ibid., 133.

> I seldom drank liquor, only beer and wine, which gave me plenty of opportunities to feel high and, often, drunk.[202]

For a time, Ames hid his addiction. He narrates for Earley:

> …my first wife seldom drank more than a glass of wine at dinner and we never drank at home at all. I would go to parties and sometimes get a definite high. The drinking got more serious in NY [New York] and on foreign trips. It wasn't boredom or loneliness that made me drink, rather the attraction was having a timeout period just for myself, when I could relax and lose myself for an afternoon or evening. I always took care to arrange these binges at times when I didn't need to work and would not be called. Typically, I would just sit in a hotel room with a book and read and drink myself to sleep, consuming most of a fifth of vodka or cognac in one sitting. I don't think anyone at the agency new about this binge drinking when I was traveling.[203]

3. Ideology/Disillusionment/Loyalty

Ames "started working for the CIA when he was sixteen, a summer stint filing records after finishing up his sophomore year in high school…."[204] However, by 1980, Ames began to lose interest in working for the CIA, stating, "All the CIA wanted to do was catch spies, it really didn't want useful intelligence."[205]

After Ames was captured, one Federal Bureau of Investigation (FBI) employee questioned how Ames could betray his friends,

> What really amazed me about Rick is that I thought he had a feeling of loyalty to the people whom he dealt with and that is the betrayal that I can't understand—the personal betrayal. I can understand why he didn't have any loyalty to the agency. I can understand how he could have lost his way so that there came a point when it didn't matter to him if he was the recruiter or the recruitee. But what I can't understand is how he lost his loyalty not only to his co-workers, such as me, but his friends, people like Sergey Fedorenko [one of the agents who was executed]! How can you ever justify betraying the people closest to you? [R. Patrick Watson][206]

---

202 Earley, *Confessions of a Spy*, 54.

203 Ibid., 112.

204 Maas, *Killer Spy*, 34.

205 Earley, *Confessions of a Spy*, 83.

206 Ibid., 85.

A friend from high school believes that overall Ames was an anxious person. She explains:

> Here is my hypothesis. Rickie is drawn to the CIA. His father worked there and he sees the agency as having a certain glamour. But then he gets into it, and he discovers that it is a government bureaucracy just like all the other government bureaucracies. Now some are good, but most are filled with time servers—people who get promoted because they have been there a long time or they have rubbed the right apple. I can see Rickie, who was always very creative but never good in a bureaucratic setting, not doing well and waking up one day and saying to himself, is this how I should spend my life? The sad thing about Rickie is that I don't think he would have had the gumption to do what any decent person would have done at that point, which is simply to get out. You see, Rickie always avoided confrontation, and I think basically that behind his mask, he is a fearful person. This is not wimpiness. Obviously he took a lot of risks being a spy. So I don't mean that. Rather it is a basic gutlessness—an inability to take his life in his own hands and take responsibility for his own actions. [Margaret "Peggy" Anderson][207]

Ames was stationed in Mexico City where he met his second wife Rosario, a Columbian citizen. As they courted, he began to recognize how alienated he felt from the United States, stating, "I feel nothing but complete revulsion for most aspects of popular culture in the United States.'"[208]

4. Security Concerns

Ames had a history of security violations, but he was rarely if ever admonished. Ames submitted notification to the CIA that he planned to live with Rosario, a necessary proclamation given her foreign citizenship. When the marriage was announced, the chief of counterintelligence recommended Ames be moved to a less sensitive job—one that did not allow access to the highest classified secrets. In common bureaucratic fashion, this concern never went further than the director of personnel, who believed it was not his decision to make. So the issue never went further.[209] At a CIA Christmas party Ames "was found drunkenly copulating with a CIA secretary on an agency desk-and on another

[207] Ibid., 113.

[208] Ibid., 128.

[209] Ibid., 129.

occasion being serviced orally."[210] He was not reprimanded for either incident. Maas describes:

> In the twenty-twenty hindsight concerning Rick in Rome, there was an avalanche of reports about Rick drinking his lunch, staggering back to his office unable to function, that he had been reprimanded (verbally) for his alcohol dependency, that he had been counseled 'in an almost sheepish way' by the station manager to seek help, that he was 'one of the worst drunks in the outfit….'[211]

5. Financial Concerns

Not only did Ames have an issue with alcohol, but he also had an issue with excessive spending. As a result of extravagant spending, Ames became stressed from excessive debt. When asked why he sold classified information he replied:

> That's a damn good question. At the time, I told myself that I was doing it for the money. And that is what I still tell people. I say, "Let's be clear about this. There is no question. I did it for the money." But now I am wondering if that is really an accurate answer. Was it just for the money? Or was getting the money just a way for me to excuse or justify what I had wanted to do all along? Why did I immediately think that I had to do something illegal? I never even thought about sitting down with a credit counselor. Why did I descend immediately into thinking of selling out my country? Why? Now that is the real question, isn't it? Why did this betrayal come so easily to me? I just don't know. Let me think.'[212]

In prison, Ames disclosed to Earley that he was motivated by fear and profit and, to a certain extent, by insecurity. He confessed, "I personally felt alienated from my own culture. I did not feel any sense of loyalty to what mass culture had become. I did not feel part of our society."[213]

> Why did I do it? I did it for the money. Period. I am not lying. I wanted the cash. But the reason I needed the money was not for the reasons most people want money. I did not want it for a new car or a new house, but rather for what it could guarantee. It seemed to be the only way for me to guarantee that the 'us' [his relationship with Rosario] I desired so

---

210 Maas, *Killer Spy*, 41.

211 Ibid., 99.

212 Earley, *Confessions of a Spy*, 136.

213 Ibid., 146.

> desperately would survive. It would make 'us' possible and, therefore, make our love a lasting one. I wanted a future. I wanted what I saw we could have together…. So you see, my turning to the KGB was actually a great act of cowardice. I decided to let the KGB worry about keeping me safe. I decided not to deal with the enormity of what I had done…it was a quick and easy way for me to get a sense of relief.[214]

He continued:

> …I have always quietly doubted myself, my own self-worth, and I was afraid to risk losing what I had. This is my innermost fear—that those who claim to love me will walk away once they see who I really am.[215] "[Money] said Rick Ames was not a failure."[216]

Duffy uses Ames's own words to describe Ames:

> Introverted and essentially a loner, in family surroundings that placed a premium on good manners, where private feelings and thoughts were not to be intruded upon, Rick found it difficult to reach out to others. If they reached out to him, however, he responded with some charm. It was a trait that would accompany him throughout his life.[217]

Duffy's analysis of Ames' relationship with Rosario contains most all of Ames' own words,

> In many respects, he's an emotionless person, but when it comes to her, it's different. There's a perverse need he had for her and she fulfilled it. He'll well up emotionally about her, and that's about all he wells up about. Of course, at that time, when he met her, she was a lot more attractive physically. He was suffering from incredible low self-esteem, having lost in effect one woman, and at his age was in sort of a midlife crisis. Then along she comes, breathing new life into him both sexually and intellectually. And between the boozing and losing his first wife and sense of worth, she made him feel he was somebody again….[218]

---

214 Ibid., 147.

215 Ibid., 148.

216 Ibid., 252.

217 Maas, *Killer Spy*, 36.

218 Ibid., 45.

Maas remarks about Ames, "But he confessed that what had propelled him was greed. Money. Rosario. He confessed, though, that he had gotten a 'rush' out of what he was doing."[219]

B. ANA BELEN MONTES

Working as a senior analyst with the Defense Intelligence Agency (DIA), Ana Belen Montes spied for the Cuban government for 16 years. Montes was openly against U.S. foreign policy towards central America.

> Counterintelligence officials say Montes had access to a range of U.S. military and intelligence secrets of interest to Havana and to terrorist groups and regimes allied with Castro. She allegedly betrayed the identity of a U.S. intelligence officer in Cuba, provided classified details about U.S. Navy war games and compromised a Special Action Program (SAP) so sensitive that she was one of only two people who knew about it. Equally if not more importantly, Montes wrote or influenced intelligence reports that might have corrupted U.S. perceptions of Cuban subversive capabilities, operations and intentions.[220]

However, Montes received only nominal financial remuneration for expenses. She was recruited by Cuban foreign intelligence officers who felt she would be sympathetic with their cause.[221] At the time of recruitment, Montes was 44 years old, single, lived alone, had few friends, and spoke fluent Spanish.[222] Montes pled guilty in 2002 and was sentenced to prison for 25 years.[223]

1. Ideology/Disillusionment/Loyalty

At the time of her sentencing, Montes said she spied purely for political and ideological reasons. She explains her reasons,

> I obeyed my conscience rather than the law. I believe our government's policy is cruel and unfair, profoundly unneighborly, and I felt morally

---

219 Ibid., 238.

220 Michael J. Waller, "Alive and Kicking," *Insight on the News*, February 18, 2002, 13.

221 Federal Bureau of Investigation, "Famous Cases and Criminals—Aldrich Hazen Ames."

222 Waller, "Alive and Kicking," 14.

223 Federal Bureau of Investigation, "Famous Cases and Criminals—Aldrich Hazen Ames."

> obligated to help the island defend itself from our efforts to impose our values and our political system on it.[224]

Montes continued to explain, quoting an Italian proverb, "all the world is one country," as she:

> defended her actions Wednesday as a necessary antidote to the 40-year-old U.S. trade embargo against Cuba, imposed by President Kennedy after the revolutionary Castro seized billions of dollars' worth of U.S. assets, stating "I did what I thought was right to counter a grave injustice," and "I hope my case in some way will encourage our government to abandon its hostility toward Cuba."[225]

Montes also refused to formally apologize for her actions, leaving prosecutors disappointed. "I felt morally obligated to help the island defend itself from our efforts to impose our values and our political system on it," she said. "We have displayed intolerance and contempt toward Cuba for most of the last four decades. We have never respected Cuba's right to make its own journey toward its own ideals of equality and justice."[226] In his book on Montes, Popkin narrates:

> She was a leftist with a soft spot for bullied nations. She was bilingual and had dazzled her DOJ [Department of Justice] supervisors with her ambition and smarts. But most important, she had top-secret security clearance and was on the inside. "*I hadn't thought about actually doing anything until I was propositioned*," Montes admitted to investigators. The Cubans "*tried to appeal to my conviction that what I was doing was right*" [emphasis added].'[227]

2. Childhood Upbringing

Montes graduated from high school with a 3.9 grade point average. But home-life proved troublesome and a growing emotional distance was occurring between Montes

---

224 Johanna Neuman, "Unrepentant Spy Gets 25 Years; 'I Obeyed my Conscience,' a Former Intelligence Agency Analyst Says of Her Work for Cuba," *Los Angeles Times*, October 17, 2002, http://articles.latimes.com/2002/oct/17/nation/na-spy17, A.1.

225 Ibid.

226 Ted Bridis, "Defiant U.S. Intelligence Analyst Sentenced to 25 Years for Spying," The Associated Press, October 17, 2002, http://www.freerepublic.com/focus/news/770647/posts

227 John Popkin, "Ana Montes Did Much Harm Spying for Cuba. Chances Are, You Haven't Heard of Her," *Washington Post*, April 21, 2013, http://www.washingtonpost.com/sf/feature/wp/2013/04/18/ana-montes-did-much-harm-spying-for-cuba-chances-are-you-havent-heard-of-her/

and her father, Alberto. “To outsiders, Alberto was a caring and well-educated father of four. But behind closed doors, he was short-tempered and bullied his children. Alberto ‘happened to believe that he had the right to beat his kids,’” Montes explained when undergoing psychological tests.[228] She expounded to her caseworker that her father “was the king of the castle and demanded complete and total obedience.”[229] Speaking to the caseworker, Montes’ “sister said child abuse began at five years of age and their father had a violent temper. ‘Ana’s mother feared taking on her mercurial husband, but as the verbal and physical abuse persisted, she divorced him and gained custody of their children.’”[230]

Montes CIA profile stated: “Ana was 15 when her parents separated, but the damage had been done. Montes’ childhood made her intolerant of power differentials, led her to identify with the less powerful, and solidified her desire to retaliate against authoritarian figures.”[231] Her “arrested psychological development” and the abuse she suffered at the hands of a temperamental man she associated with the U.S. military “increased her vulnerability to recruitment by a foreign intelligence service….”[232] Montes’ sister commented that even in childhood, “She wasn’t one that wanted to share things or talk about things.”[233]

As a result of her experiences Montes only confidents were her Cuban handlers. An article by Popkin explains:

> At the beginning, the Cubans provided enough of a social life. “*They were emotionally supportive. They understood my loneliness*,” Montes told investigators. But as she turned 40, Montes became despondent. “*I was finally ready to share my life with someone but was leading a double life, so I did not feel I could live happily*,” she revealed [emphasis added].[234]

---

[228] Ibid.

[229] Ibid.

[230] Ibid.

[231] Ibid.

[232] Ibid.

[233] Ibid.

[234] Ibid.

When contact was briefly interrupted, Montes' experienced severe emotional trauma. Popin remarks in his article, "CIA-led psychologists would later conclude that the isolation, lies, and fear of capture had triggered borderline obsessive-compulsive traits."[235]

Montes's sister wrote of her betrayal,

> You betrayed your family, you betrayed all your friends. Everyone who loves you was betrayed by you. You betrayed your co-workers and your employer, and you betrayed your nation. You worked for an evil megalomaniac who shares or sells our secrets to our enemies.[236]

Her sister believes Montes ultimately committed unauthorized disclosure to obtain power over other people, in order for her to feel powerful. Rather than seeking power, Montes may have become emotionally attached to her Cuban handlers to fulfill a feeling of security that she did not have as a child.

Montes was highly successful at work, lived modestly; she did not suffer from any known addiction, nor did she have financial problems. Additionally, she did not have a history of security concerns aside from two security interviews in which she acknowledged her disagreement with U.S. foreign policy towards Cuba. The foreign policy issue was an emotional one for her.[237]

C. CHELSEA (FORMERLY BRADLEY) MANNING

While serving as an intelligence analyst in the U.S. Army in Iraq in 2009 and 2010, Chelsea Manning released more than 700,000 classified files, combat videos and diplomatic cables to Wikileaks, an online anti-secrecy group. Her motivation appears to be disillusionment with the world affairs of the U.S. government about what she learned

---

235 Ibid.

236 Ibid.

237 Scott W. Carmichael, *True Believer: Inside the Investigation and Capture of Ana Montes, Cuba's Master Spy* (Annapolis, MD: Naval Institute Press, 2007), 20.

in Iraq and a resultant questioning of U.S. foreign policy.[238] Arrested in May 2010, Manning was found guilty of 20 of 21 charges in 2013 and sentenced to 35 years in prison.

1. Ego and Intellect

Manning was highly computer literate, but a former supervisor said she was weak on the social side of analyzing intelligence.[239] She currently suffers from serious emotional problems that were also prevalent during her youth (feeling profoundly alienated and fearful about her secret). She has always been a loner, physically weak, and suffered from a stunted personality.

2. Ideology/Disillusionment/Loyalty

From written conversations with the computer hacker who reported her to authorities, Manning talked about feeling isolated, suffering from mental instability, and from gender identity disorder.[240] Working as an intelligence analyst in Iraq, Manning:

> began to become depressed with the situation that [the United States became] increasingly mired in year after year. [She] felt that [the United States] were risking so much for people that seemed unwilling to cooperate with us, leading to frustration and anger on both sides.[241]

She seemed to be losing connections with those closest around her. She no longer communicated with her father and her relationship with her boyfriend had ended.

Gender identity issues were a major source of stress for Manning. She came out as transgender and in an email sent to her supervisor in 2010 stating she joined the Army

---

238 After his conviction, Manning declared he wanted to live as a woman. Brad Knickerbocker, "Bradley Manning Trial Closing Arguments Ask: Why Did He do It?" *The Christian Science Monitor* (Boston), July 25, 2013, http://www.csmonitor.com/USA/Justice/2013/0725/Bradley-Manning-trial-closing-arguments-ask-Why-did-he-do-it

239 Paul D. Shinkman, "Defense Paints Bradley Manning as Misguided" *U.S. News and World Report*, July 9, 2013, http://www.usnews.com/news/articles/2013/07/09/defense-paints-bradley-manning-as-misguided

240 Elspeth Reeve, "A Portrait of the Mind of Bradley Manning," *The Wire*, August 14, 2013, http://www.thewire.com/national/2013/08/portrait-mind-bradley-manning/68341/

241 Richard A. Serrano, "Private's Trial, Government's Test: Bradley Manning Court Martial in the WikiLeaks Case Could Embarrass the Keepers of America's Secrets," *The Los Angeles Times*, June 2, 2013, A 10.

to "to get rid of it."[242] "You put him in this hyper-masculine environment, if you will, with little support and few coping skills—the pressure would have been difficult to say the least," testified an Army mental health counselor who counseled Manning in Iraq. U.S. Army Captain Michael Worsley, a psychiatrist who interviewed Manning after her arrest, believes she has symptoms of fetal alcohol syndrome and Asperger syndrome, as well as narcissistic traits that become worse with stress. Manning was "acting out his grandiose idealation," and was convinced that she could change the world.[243]

Manning, frustrated by countries acting only in self-interest, told the court she leaked the documents to start a public debate about the role of the United States military and foreign policy.[244] Manning "found the machinations of first world governments 'exploiting' third world ones to be disgusting, and hoped 'worldwide discussion, debates, and reforms' would result from the release of the documents she passed on."[245] At her trial, her statement read:

> I understand that my actions violate the law. It was never my intent to hurt anyone. I only wanted to help people. When I chose to disclose classified information, I did so out of a love for my country and a sense of duty for others.

3. Security Concerns

When stationed at Fort Huachuca, Arizona in 2008, Manning was reprimanded for posting YouTube videos that revealed sensitive information.[246] Moving to Fort Drum in August to train for deployment, Manning was again reprimanded for yelling at fellow

---

242 Margaret Hartmann, "Ahead of His Sentencing, Bradley Manning Says, 'I'm Sorry I Hurt the United States,'" *New York Magazine*, August 15, 2013, http://nymag.com/daily/intelligencer/2013/08/bradley-manning-im-sorry-i-hurt-the-us.html

243 Ibid.

244 "WikiSecrets," *Frontline*, May 24, 2011, http://video.pbs.org/video/1946795242/

245 Alexis C. Madrigal, "Bradley Manning, the Person: The Making of the World's Most Notorious Leaker," *The Atlantic*, July 13, 2011, http://www.theatlantic.com/technology/archive/2011/07/bradley-manning-the-person-the-making-of-the-worlds-most-notorious-leaker/241920/

246 Denver Nicks, "The inside Story of the Oklahoman behind the Biggest Military Intelligence Leak Ever," *Way Back Machine* [blog] September 23, 2010, https://web.archive.org/web/20110429142813/http://thislandpress.com/09/23/2010/private-manning-and-the-making-of-wikileaks-2/

soldiers and throwing furniture.[247] Becoming increasingly isolated while deployed in 2009, Manning began to act out. After striking another soldier, she was demoted from specialist to private first class.[248] Prior to the repeal of "don't ask, don't tell," Manning was posting photos with her boyfriend and attending gay rights rallies.[249] One week after the breakup with her boyfriend, Manning was found in a fetal position, clutching a knife, having etched "I want" into a chair.[250]

4. Childhood Upbringing

Manning grew up in rural Oklahoma, the child of alcoholic, abusive parents, and possibly is a victim of fetal alcohol syndrome.[251] As a child, she was high strung and extremely intelligent.[252] She considered herself "very effeminate" and "very intelligent."[253] By kindergarten, she was teased at school and at home. Other students called her a "girly boy" or teacher's pet." She retreated into her room to learn things. She explained, "My favorite things growing up were reading my encyclopaedia, watching PBS (the only channel I could get on my TV), building with legos, and playing on my dad's hand-me-down computers."[254]

Manning's mother filed for divorce after her father threatened her with a shotgun for making too much noise.[255] She later attempted suicide. Upon recovery, she and Manning moved to her mother's hometown in Wales, United Kingdom. Several years later, Manning returned to the United States after her mother began having strokes.[256] By this time, Manning had come to terms that she was a homosexual. Her father kicked her

---

247 "WikiSecrets," *Frontline*.

248 Nicks, "The Inside Story of the Oklahoman."

249 "WikiSecrets," *Frontline*.

250 Ibid.

251 Reeve, "A Portrait of the Mind of Bradley Manning."

252 Nicks, "The Inside Story of the Oklahoman."

253 Madrigal, "Bradley Manning, the Person."

254 Ibid.

255 Ibid.

256 Ibid.

out of the house for being gay and after a series of failed jobs, she joined the Army in October 2007, although the "don't ask, don't tell" policy was in effect.[257]

D. BRIAN REGAN

Brian Regan worked as a defense contractor for the National Reconnaissance Office (NRO). His intent was to collect and sell classified information concerning U.S. reconnaissance satellites to Iraq, China, and Libya.[258] However, unable to find a buyer for the large volume of classified information he had amassed, Regan buried it. At his trial, officials displayed piles of boxes marked "top secret that contained estimated 10,000–20,000 pages of sensitive material, including documents, slides, and videos, some of which pertain to satellites and early warning systems."[259] In 2003, he was found guilty of attempted espionage and gathering national defense information and sentenced to life in prison.[260]

1. Ego and Intellect

Although challenged by dyslexia, Regan illustrated a high level of intelligence by overcoming that disability and undertaking a long-term plan to sell U.S. classified information. He stole thousands of documents, buried them in 19 locations in Maryland and Virginia, and developed a "series of codes, marked trees, and carefully buried packages that would allow agents of China, Libya, or Iraq to directly retrieve the materials secretly."[261] In the Air Force, Regan had been trained in cryptanalysis and to use that skill to create manual code and ciphers; he was able to maintain a guide to where the documents were hidden.

---

257 Ibid.

258 Suzann Chapman, "Retired Airman Faces Death Penalty in Espionage Case," *Air Force Magazine* 85, no. 6 (2002): 19.

259 "Convicted Spy Buried Sensitive U.S. Defense Documents in 19 Locations," *Information Management Journal* 37, no. 6 (November 2003), http://www.freepatentsonline.com/article/Information-Management-Journal/111011464.html, 13.

260 "Brian Patrick Regan," Wikia Military, accessed December 9, 2014, http://military.wikia.com/wiki/Brian_Patrick_Regan

261 "Convicted Spy Buried Sensitive U.S. Defense Documents in 19 Locations," *Air Force Magazine*, 13.

2. Ideology/Disillusionment/Loyalty

Regan was disillusioned about his and his family's financial future. In letters to foreign government dictators, he detailed his anger at the small pension he would receive after a 20-year Air Force career compared to the millions celebrities made after just a few years.[262] He was amassing debt as his wife was still in college and they had had four children to raise.

3. Financial Concerns

Regan is attributed to having:

> credit card debts of $117,000 when he drafted a letter to [Saddam Hussein] offering to sell U.S. intelligence for $13 million. He made similar offers to Chinese and Libyan officials, though… he never actually passed any information. Regan was carrying information with the coded coordinates of Iraqi and Chinese missile sites, the missiles that were stored there, and the dates the information was obtained. He also had the addresses of the Chinese and Iraqi embassies in Switzerland and Austria in his wallet and tucked into his right shoe.[263]

Regan was arrested at Dulles Airport in August 2001 as he was preparing to board a flight to Zurich,[264] although he had told his colleagues that he was taking his family to Disney World.[265]

4. Childhood Upbringing

Regan was born dyslexic and "grew up feeling stupid, comparing himself to other kids because of the grades he got," according to a psychiatrist who interviewed and counseled him in jail. He was also socially awkward; however, upon joining the Air Force he was able to improve his education listening to audiobooks.[266]

---

[262] Herbig, *Changes in Espionage by Americans: 1947–2007*, 33–34.

[263] "Man Receives Life Sentence in Espionage Case," *Richmond Times Dispatch*, March 21, 2003, A3.

[264] "Brian Patrick Regan," Wikia Military.

[265] Kevin Whitelaw, "Surfing for Secrets: A(nother) Spy Caper," *U.S. News and World Report* 131, no. 8 (September 2001), 20.

[266] Yudhijit Bhattacharjee, "Hide and Seek," *Wired* 18, no. 2 (February 2010), http://www.wired.com/2010/01/ff_hideandseek/

E. BRYAN UNDERWOOD

A former U.S. Marine, Bryan Underwood, attempted to pass classified national security information to China while working as a contract security guard at a U.S. consulate under construction in China.[267] Arraigned in September 2011, Underwood was sentenced for a period of nine years[268] in August 2012 of attempting to communicate national defense information to a foreign government.[269] That information would have given China undetected access to the consulate, to include the secure areas, by providing photographs of the construction, a list of security upgrades, and locations of surveillance security cameras. He never got to put on paper his mental plan of where listening devices could be installed.[270]

1. Financial Concerns

In March 2011, Underwood became panicked about his financial situation when his stock brokerage account fell from $68,813 to negative $89,624 in two months.[271] It was then that Regan tried to contact the Chinese Ministry of State Security to offer the classified photographs, information, and access to U.S. facilities for $3 million to $5 million.[272]

2. Childhood Upbringing

At sentencing, the judge cited Underwood's mental problems and troubled childhood as reasons for giving him a more lenient sentence. Underwood himself said he

---

267 "U.S. Consulate Guard Admits to Selling Secrets to China," *The Irish Times Limited*, August 31, 2012, 12.

268 Lawrence Hurley, "Bryan Underwood, Ex-Security Guard at U.S. Consulate in China, Sentenced to 9 Years for 'Half-Baked Treason,'" *The World Post*, March 5, 2013, http://www.huffingtonpost.com/2013/03/05/bryan-underwood-attempted-treason-sentence_n_2812274.html

269 Federal Bureau of Investigation Washington Field Office, "Former U.S. Consulate Guard Sentenced to Nine Years in Prison for Attempting to Communicate National Defense Information to China," March 5, 2013, http://www.fbi.gov/washingtondc/press-releases/2013/former-u.s.-consulate-guard-sentenced-to-nine-years-in-prison-for-attempting-to-communicate-national-defense-information-to-china

270 Ibid.

271 Serrano, "Private's Trial, Government's Test," A.11.

272 "U.S. Consulate Guard Admits to Selling Secrets to China," *The Irish Times Limited*, 12.

was a paranoid schizophrenic undergoing mental health treatment,[273] but this could not be substantiated through additional literature.

F. GREG WILLIAM BERGERSEN

While working as a weapons systems policy analyst at the Department of Defense, Greg Bergersen sold classified national defense information to Tai Kuo, a naturalized citizen from Taiwan who was also an agent of the People's Republic of China.[274] The information, primarily related to the sale of military sales to Taiwan[275] and U.S. military communications security, was then passed on to China. Kuo cultivated a friendship with Bergersen, giving him gifts, cash payments, dinners, and money for gambling trips. He also led Bergersen to believe that he would involve him with a company selling U.S. defense technology to Taiwan after Bergersen retired from government service.[276] In February 2008, Bergersen was charged with conspiracy to disclose national defense information to persons not entitled to receive it[277] and pled guilty to the conspiracy charge in March 2008. He was sentenced to 57 months in prison.[278]

1. Ideology/Disillusionment/Loyalty

Bergersen believed Kuo worked the Taiwanese government[279] and the information was being sold to Taiwan, rather than China, which does not recognize

---

273 Hurley, "Bryan Underwood, Ex-Security Guard at U.S. Consulate in China."

274 United States District Court for the Easter District of Virginia, Alexandria Division: United States of America v. Tai Shen Kuo, a/k/a Tai Kuo, Kuo Tai Shen, Gregg William Bergersen, and Yu Xin Kang, a/k/a Kang Yu Xin, Katie, Defendant" (Case No. 1:08mj, 2008), http://fas.org/irp/ops/ci/kuo-affidavit.pdf

275 Federal Bureau of Investigation, "Spies on the Inside: Foreign Intrigue on American Soil," February 14, 2008, http://www.fbi.gov/news/stories/2008/february/espionagecases_021408

276 "U.S. Department of Justice: New Orleans Businessman Pleads Guilty to Espionage Charge Involving China," *Asia Business Newsweekly*, May 26, 2008, http://www.justice.gov/archive/opa/pr/2008/May/08-nsd-411.html, 59.

277 Stéphane Lefebrve, "The PRC's Compromise of U.S. Government Information and Technologies, *International Journal of Intelligence and Counterintelligence* 22, no. 4 (September 3, 2009): 656.

278 Jim Kouri, "Defense Department Official Imprisoned for Espionage," Renew America, July 16, 2008, http://www.renewamerica.com/columns/kouri/080716

279 Bill Walsh, "Three Arrested in Chinese Spy Plot: Pentagon Official Accused of Passing Weapons Secrets to Local Businessman and Recent Immigrant Cash, Poker Chips Bought Arms Sale Details, FBI Says," *Times-Picayune*, February 12, 2008, 1.

Taiwan as an independent country. Regardless, he knew he was committing a crime. As was noted in an article for *Biotech Business Week*, "Mr. Bergersen predicted he would go to jail if anyone discovered he was unlawfully providing classified information to a foreign government."[280] According to a wiretapped conversation with Kuo, Bergersen said "If [the classified information] ever fell into the wrong hands, and I know it's not going to, then I'd be fired for sure. I, I'd go to jail."[281]

2. Financial Concerns

While monetary gains seem to be the main motive for selling secrets, Bergersen appears to have received only minimal payment. In July 2007, Kuo placed $3,000 in Bergersen's shirt pocket in order to access the details of five years' worth of planned weapons sales to Taiwan. The papers had jagged edges where Bergersen had removed the "classified" markings.[282] Bergersen has acknowledged receiving $3,000 in cash for gambling and show tickets worth $875 in Las Vegas in February 2008.[283] Bergersen's long-term goal that was never achieved was to become a partner/co-owner of a company selling U.S. military technology to Taiwan.

G. HASSAN ABU-JIHAAD (FORMERLY PAUL R. HALL)

While serving as a U.S. Navy signalman aboard a warship in 2001, Hassan Abu-Jihaad ("father of jihad" in Arabic),[284] formerly known as Paul R. Hall, was a homegrown extremist who shared details of ship vulnerabilities and scheduled movements of several warships with Al-Qaeda.[285] Abu-Jihaad also sent messages supporting Osama bin Laden, praising the attack on the United States ship (USS) *Cole* in

---

280 "U.S. Department of Justice: Former Defense Department Official Sentenced to 57 Months in Prison for Espionage Violation," *Biotech Business Week*, July 28, 2008, http://www.justice.gov/archive/opa/pr/2008/July/08-nsd-604.html, 1785.

281 Walsh, "Three Arrested in Chinese Spy Plot," 1.

282 Bill Walsh, "Arms Analyst Admits Role in Spy Ring: He'll Aid in Prove of 2 N.O. Residents," *Times-Picayune*, April 1, 2008, 3.

283 Ibid.

284 Herbig, *Changes in Espionage by Americans: 1947–2007*, 53.

285 Federal Bureau of Investigation, "Passing Secrets at Sea: To Terrorists, No Less," March 10, 2008, http://www.fbi.gov/news/stories/2008/march/secrets031008

October 2000 that killed 17 Americans while stationed in the port of Yemen. Over the Internet, he ordered various materials supporting jihad.[286] Abu-Jihaad was arrested in March 2007 and charged with materially aiding terrorism with intent to kill U.S. citizens, as well as transmitting classified information to those not authorized to receive it.[287] In March 2008, he was tried and convicted of providing material support to terrorists and of disclosing classified national defense information. He was sentenced to 10 years in prison.[288]

1. Ideology/Disillusionment/Loyalty

While stationed on the USS *Benfield*, Abu-Jihaad communicated with anonymous jihadists over the Azzam Publications website (an English language Islamist website). He expressed enthusiasm for Islam, as well as writings on terror tactics:

> [Referring to Islamist fighters in one of his videos] with their only mission in life to make Allah's name and mission supreme all over the world, I want to let it be known that I have been in the middle east for almost a total of 3 months [that is, while onboard the USS *Benfield*]. For those 3 months you can truly see the effect of this psychological warfare taking a toll on junior and high ranking officers… [they were] running around like headless chickens very afraid (United States District Court of Connecticut, Warrant, 2007).[289]

In one email he called the attack on the USS *Cole* in 2000 a "martyrdom operation" and praised "the men who have brong (sic) honor ... in the lands of jihad Afghanistan, Bosnia, Chechnya, etc."[290]

2. Childhood Upbringing

Paul R. Hall was raised in San Bernardino, California and joined the U.S. Navy at 19. In 1997, Hall converted to Islam, taking the name Hassan Abu-Jihaad.[291]

---

286 Ibid.

287 Herbig, *Changes in Espionage by Americans: 1947–2007*, 53.

288 Ibid., 53.

289 "Ex-Sailor Found Guilty of Leaking Ship Movements," *IPT News*, March 6, 2008, http://www.freerepublic.com/focus/f-news/1981476/posts

290 Ibid.

H. ROBERT HANSSEN

Working as an intelligence analyst for the Federal Bureau of Investigation (FBI), Robert Hanssen provided classified information to Soviet and Russian intelligence officials between 1979 and 2001. Arrested in 2001, Hanssen was charged with espionage and conspiracy to commit espionage. He was convicted of 15 counts of espionage the same year and was sentenced to 15 consecutive life sentences.[292] According to the 2003 Department of Justice (DOJ) report, Hanssen's initial decision to engage in espionage

> arose from a complex blend of factors, including low self-esteem and a desire to demonstrate intellectual superiority, a lack of conventional moral restraints, a feeling that he was above the law, a lifelong fascination with espionage and its trappings and a desire to become a "player" in that world, the financial rewards he would receive, and the lack of deterrence—a conviction that he could "get away with it."[293]

1. Ego and Intellect

Highly educated and a good student, Hanssen resented not being properly recognized and promoted because of his skills. Additionally, he longed to prove to his colleagues that he was cleverer than they thought.[294] His egotistic tendencies were demonstrated when arrested in February 2001 and he asked the FBI agents, "What took you so long?"[295] He was known for wearing dark suits, and co-workers referred to him as Dr. Doom. He sensed he was never going to be promoted to one of the top jobs in the FBI, and he resented it. He was not one of the boys.[296]

---

[291] Defense Personnel Security Research Center, *Espionage and Other Compromises of National Security. Case Summaries from 1975 to 2008* (Monterey, CA: Defense Personnel Security Research Center, 2009), 1.

[292] *Wikipedia*, "Robert Hanssen," accessed January 22, 2015, http://en.wikipedia.org/wiki/Robert_Hanssen

[293] U.S. Department of Justice, *A Review of the FBI's Performance in Deterring, Detecting, and Investigating the Espionage Activities of Robert Philip Hanssen*, August 2003, accessed May 17, 2013, http://www.justice.gov/oig/special/0308/final.pdf, 10.

[294] Frederick P. Hitz, "The Truth of Espionage is Stranger than Fiction," *Intelligence and National Security* 23, no. 1 (January 2009): 56. 55–60.

[295] James Bauerle, "Golden Eye Redux," *The Banking Law Journal* 120, no. 3 (2003): 273. 266–278.

[296] Hitz, "The Truth of Espionage is Stranger than Fiction," 56.

The Russian intelligence officers were able to play to Hanssen's "insecurity, vanity, desire for power and control, and yearning for friendship," stroking his ego to obtain United States' classified secrets. In 2003 article, Bauerle remarked,

> For his part, Hanssen compartmentalized his thoughts and feelings, reasoning that he had betrayed no one, having instead expanded the circle of his friends to include those who played the intelligence game at a higher level than the FBI, just as he did.[297]

2. Addiction

Hanssen appears to have had a sexual deviancy involving kinky sex. When his closest friend went overseas with the U.S. Army, Hanssen sent him nude photos of his wife and later video-tapes of his wife and him having sexual intercourse. His wife was not aware this was happening.[298] Eventually, Hanssen set up a video camera in their bedroom so when his friend visited, he could watch the Hanssens in their bedroom. This was done at Hanssen's urging, his friend never requested to see intimate encounters. Believing that his friend's life was empty since he did not have a child, Hanssen suggested drugging his wife with a "date rape" drug so his friend could impregnate her.[299] Hanssen eventually befriended a local stripper, whom he showered with gifts, including expensive jewelry, a Mercedes, a laptop computer, and cash.[300]

3. Ideology/Disillusionment/Loyalty

After marriage, Hanssen converted to Catholicism and became a member of Opus Dei, a secretive Catholic organization. According to Baumann:

> Opus Dei…members lead a kind of double life; to the world, they are successful doctors or lawyers, distinguished only by their professional skills and autonomy; off the job they must not only engage in an intense

297 Bauerle, "Golden Eye Redux," 273.

298 Hitz, "The Truth of Espionage is Stranger than Fiction," 56.

299 David Wise, *Spy: The Inside Story*, 260.

300 Ibid., 144–150.

> life of prayer (all to the good) but be strictly accountable to those above them in 'the work' (more problematic).[301]

This double-agent quality may have appealed to Hanssen, whose career had been mainly in counterespionage. In his book, Bauman muses:

> Professionally, he seems to have put great stock in his intellectual and moral superiority over those around him. Hanssen's contempt for the bungling of his fellow FBI and CIA agents seems to have been linked to his disdain for the godlessness, materialism, and sexual license of American society.[302]

Hanssen tried to recruit others to become Roman Catholic, and he was vocal regarding anti-Communism and licentious behavior. Hanssen "preached to all who would listen that man is lost without religion, which is why the Soviet Union—run by godless Communists—would ultimately fail."[303] Yet here was a man who did not honor what the Roman Catholic Church taught, was supporting those he calls godless, and practicing sexually deviant behavior.

Hanssen himself speaks of his psychological conflicts. In March 2000, he wrote to his handlers,

> I have come about as close as I ever want to come to sacrificing myself to help you. Conclusion: One might propose that I am either insanely brave or quite insane. I'd answer neither. I'd say, insanely loyal. Take your pick. There is insanity in all the answers.[304]

4. Security Concerns

Hanssen's knowledge of FBI culture allowed him to practice unauthorized disclosure without detection. A DOJ report documents:

> First, Hanssen was capable of being uniquely reactive to counterintelligence investigations because of his placement within the FBI counterintelligence bureaucracy. Second, Hanssen was able to alter his

---

[301] Paul Baumann, "Agent Hanssen: The Spy Who Came in from the Fold," *Commonweal*, March 23, 2001, 8.

[302] Ibid.

[303] Bauerle, "Golden Eye Redux," 270.

[304] Richard Willing, and Traci Watson, "FBI Portrays Robert Hanssen's Double Life: A 15-Year Paradox," February 21, 2001, *USA Today*, A.1.

> contact procedures with his Russian associates whenever he felt that he was close to being caught; he was even able to search for his own name within the FBI internal database to monitor whether he was the subject of any investigation.[305]

In his book *Spy*, Wise notes, "Third, Hanssen knew how to avoid movement within the FBI bureaucracy that would have subjected him to polygraph examinations."[306]

5. Financial Concerns

Hanssen had financial motivators for selling secrets, although he continued to live within his means. He had a large family to provide for. In November 1985, Hanssen engaged Russian intelligence officers and volunteered to provide information "for money, a few diamonds for his children and good will."[307] Overall, Hanssen received more than half a million dollars in cash and $50,000 in diamonds. He was also told that $800,000 waited for him in a Russian bank account. It appears he harbored a fantasy of retiring from the FBI and teaching college courses in Moscow.[308] However, Hanssen recognized the difficulty of sudden affluence, writing on his Russian contact on March 3, 1986:

> As far as more funds are concerned, I have little need or utility for more than the $100,000. It merely provides a difficulty since I cannot spend it, store it or invest it easily without (tripping the FBI's) "drug money" warning bells. Perhaps some diamonds as security to my children and some good will so that when the time comes, you will accept (my) senior services as a guest lecturer. Eventually, I would appreciate an escape plan. Nothing lasts forever.[309]

6. Childhood Upbringing

Hanssen's father was a harsh disciplinarian and verbally and physically abusive. He continuously berated Hanssen, telling him he would never amount to anything. While his father hoped Hanssen would become a doctor, Hanssen dropped out of dental school

---

[305] U.S. Department of Justice, *A Review of the FBI's Performance*.

[306] Wise, *Spy: The Inside Story*, 177.

[307] Willing, and Watson, "FBI Portrays Robert Hanssen's Double Life," A.1.

[308] Ibid.

[309] Ibid.

and pursued a master's of business administration before entering into law enforcement. As a result of the abuse, Hanssen's court-appointed psychoanalyst believed Hanssen possessed an enormous fear of being perceived by his wife and family as inadequate or a failure. He craved the financial success his father wished of him and feared that he had not measured up.[310] As said by the psychoanalyst, "the prime motive for his spying was to preserve his image in Bonnie's [his wife] eyes as a good provider."[311]

I. JOHN WALKER

In 1968, while serving in the U.S. Navy, John Walker walked into the Soviet Embassy in Washington, DC and offered to sell classified nuclear information. Walker said later "the theft was an impulsive act caused by his deep depression over his marital and financial problems."[312] During the 18-year period in which he sold information, Walker enlisted his brother, his best friend, and his son to steal classified information for him. Walker's ex-wife and daughter eventually went to authorities to discuss the relationship Walker had with the Russians. In May 1985, Walker was arrested. He pled guilty to espionage and was sentenced to life in prison.[313]

1. Ego and Intellect

When Walker was given access to classified nuclear information, he began to wonder what it might be worth. Because of the constant awareness briefings to protect classified information, he felt that it might be worth something to the Russians.[314] Growing up with a troubled childhood and later a troubled marriage, he was determined to move quickly up the enlisted ranks in the Navy.

---

[310] Hitz, "The Truth of Espionage is Stranger than Fiction," 56.

[311] Wise, *Spy: The Inside Story*, 273.

[312] Pete Earley, *Family of Spies: Inside the John Walker Spy Ring* (New York: Bantam Books, 1989), 68.

[313] John Prados, "The Navy's Biggest Betrayal," *Naval History Magazine* 24, no. 3 (June 2010): 36–45, http://www.usni.org/magazines/navalhistory/2010-06/navys-biggest-betrayal

[314] Earley, *Family of Spies: Inside the John Walker Spy Ring*, 60.

Walker befriended people who admired him and whom he felt he could manipulate,[315] allowing for feelings of greater self-worth. His Russian handler was able to stroke his ego, telling him, "You are the most experienced, the very best."[316]

Walker was concerned about being able to undergo scrutiny during his security clearance reinvestigation since he was already selling secrets to the Soviets. Therefore, he resourcefully decided to forge his own security clearance. Comparing his and another sailor's paperwork, he noticed the only difference was the FBI stamp on the completed file. Walker traced the stamp, drove to an office supply store and paid $2.97 for a duplicated stamp. He was able to forge his paperwork and did not have to undergo periodic reinvestigation.[317]

Upon his arrest, Walker was incensed his spying skills were not used by the United States. He fumes: "Here I was, a person who had run a successful, perhaps the most successful spy ring in the nation's history, and all these bastards were worried about was getting out a goddamn press release. Getting public attention was more important than using me as a double agent."[318]

2. Addiction

Born to an alcoholic father, Walker also became addicted to alcohol and often used drugs. It is remarkable Walker was able to function as a spy at such a high level given the frequency he was under the influence of alcohol or drugs.

3. Ideology/Disillusionment/Loyalty

About becoming a spy, Walker explains:

> I decided that if I was going to be a spy, and I clearly was going to be one, then I would be the best damn spy there ever was, and that meant giving them everything. And that's exactly what I did.[319]

---

[315] Ibid., 109.

[316] Ibid., 6.

[317] Ibid., 132–133.

[318] Ibid., 14.

[319] Ibid., 82

> I really went through several periods as a spy. In the beginning, I felt like I was going to be caught any minute. There was a lot of fear, but after a couple years, I got into a what-the-fuck-is-happening mode. How can this be—that I'm not being arrested? It just didn't make any sense that I hadn't been captured, Then, after I'd been in California for a while, I began to enjoy myself. There was a certain thrill to it all and a metamorphosis began to take place. I began to realize that the FBI is not like it is on television. You see, the FBI doesn't really do any investigating. The FBI is not powerful at all because its agents are really just bureaucrats and they have the same inherent ineptitude of all government bureaucrats. All they do is spend their days waiting for some snitch to call them and turn someone in.[320]

Walker eventually came to feel that sharing information with the Russians prevented another world war. He said,

> I really didn't harm the country. Lots of people do it [spy]. In fact, the material I provided them probably avoided World War III, because the information was so good the Soviets were convinced we were as strong as we said we were. That's why they never attacked us, and never will.[321]

4. Security Concerns

Walker (not his brother or best friend) received security clearance reinvestigations[322] and Walker forged his own background investigation at one time. Walker had serious financial debt, but once he started selling secrets he maintained a lavish lifestyle. When queried about his lavish lifestyle, he attributed his wealth to a side restaurant/bar business, which actually was heavily mortgaged.[323] His charismatic personality convinced co-workers that his business was doing well. However, even when some began to realize something was wrong, noting, for example, Walker seemed nervous and flush with money and held a security clearance, he was never investigated.[324]

---

[320] Ibid.,, 105.

[321] Robert W. Hunter, and Lynn Dean Hunter, *Spy Hunter: Inside the FBI Investigation of the Walker Espionage Case* (Annapolis, MD: Naval Institute Press, 1999), 188–189.

[322] Sarbin, Carney, and Eoyang, *Citizen Espionage*, 59–60.

[323] Earley, *Family of Spies: Inside the John Walker Spy Ring*, 87.

[324] Ibid., 101.

5. Financial Concerns

When interviewed, Walker stated, "I became a spy because I needed the money."[325] He eventually asked the Russians to consider giving him a $1 million payment in return for a steady supply of documents during the next 10 years.[326] Upon his initial approach to the Russian embassy, the Russian intelligence officer asked if Walker came for political or financial reasons," and Walker responded, "Purely financial. I need the money."[327]

Walker's desire to live a lavish lifestyle overrode his responsibility to protect national security information. His greed and ego overruled caution even moments before his arrest. Rather than destroy instructions on where to drop a package of information and receive a $200,000 payment, Walker was apprehended with the instructions.[328]

6. Childhood Upbringing

Walker had a troubled upbringing. His life was greatly altered after his father was in a serious car accident and no longer able to adequately support his family. His father was a severe alcoholic who physically abused his wife and children to the point where Walker plotted to kill his father to end the family's suffering. His best friend described Walker's mother as "cold and distant and [Walker] complained that she hadn't spent much time with him as a boy."

As a teen, Walker became involved in petty burglaries and robberies. He joined the Navy as an option instead of going to prison for one robbery. The failures of his father and the lack of attention from his mother had a serious effect on Walker. He was determined to provide for his family (wife and children)[329] and was insistent he was not going to end up destitute like his father.[330]

---

[325] Ibid., 17.

[326] Ibid., 11.

[327] Ibid., 76

[328] Ibid., 7.

[329] Ibid. 139.

[330] Ibid., 67.

J. JONATHON POLLARD

While working for the U.S. Navy as an intelligence specialist, Jonathon Pollard sold classified national security information to Israel. Arrested outside of the Israeli Embassy while trying to seek asylum in November 1985, Pollard pled guilty to conspiracy to deliver national defense information to a foreign government and was sentenced in 1987 to life in prison. He admitted to providing Israel with reconnaissance images of the Palestine Liberation Organization (PLO) headquarters in Tunisia, details of Iraqi and Syrian chemical-warfare production capabilities, U.S intelligence assessments of operations planned by a PLO unit against Israel, and information regarding Soviet arms shipments to Syria and other Arab states.[331] Pollard was not remorseful upon his capture and subsequent conviction and incarceration. The Federal Bureau of Prisons reviewed his correspondence and discovered that:

> on three occasions [the] defendant included extensive classified information in letters to his wife, and more recently in a letter to an attorney/author, who has written critically of the sentence imposed by this court and from whom [the] defendant has sought assistance on the public relations aspects of his case.[332]

Pollard continues to actively campaign for his own release. Between 2013 and 2014, President Obama's administration underwent talks with Israel to exchange Pollard for the release of Palestinian prisoners.

1. Ego and Intellect

Olive describes Pollard as possessing a sense of inflated importance and a keen desire for recognition.[333] At first, he was an exceptional employee receiving outstanding performance reports, but became less interested in his assigned work and more eager to work on projects he found personally interesting. A report by Olive describes Pollard's performance:

---

[331] Wolf Blitzer, "Pollard: Not a Bumbler, but Israel's Master Spy," *Washington Post*, February 15, 1987, http://www.jonathanpollard.org/7890/021587.htm

[332] Ronald J. Olive, *Capturing Jonathan Pollard: How One of the Most Notorious Spies in American History Was Brought to Justice* (Annapolis, MD: Naval Institute Press, 2006), 234–235.

[333] Ibid., 13.

> He failed to meet deadlines. He ignored administrative paperwork. He complained about his work being extensively edited. He even questioned the professional competence of his immediate supervisors, expressing his dissatisfaction to his peers and those above his supervisors in the chain of command. Oddly, he continued to receive excellent performance reports.[334]

Pollard supplied the Israelis thousands of classified documents each month, yet received no security training and had no knowledge of the workings of foreign intelligence.[335] However, his ego led him to believe the Israelis would rescue him if he ever got into trouble. On the night of his arrest, Pollard felt since he was Jewish if he made it to the grounds of the Israeli embassy, sovereign territory, the Israelis would protect him from prosecution and relocate him to Israel.[336]

Once arrested, Pollard bragged to the FBI agent, "You botched it! You thought this was a Soviet bloc operation, didn't you?"[337] Upon Pollard's decision to decline the presence of an attorney, one interviewer reflected:

> Here was a guy who had admitted to espionage and just tried to gain asylum in the Israeli embassy, who was under arrest and in serious trouble, yet his reaction was one of overbearing cockiness. Pollard showed no remorse for anything. It was as if he were saying, I certainly fooled you, you idiots.[338]

A former FBI agent who worked the case believes Pollard committed espionage for recognition, rather than greed or ideology. Describing Pollard as intellectually arrogant and cocky, the agent also saw a desperate, childlike craving for recognition in him. Pollard stated that in giving secrets to the Israelis, "[it] made him dream of being a hero in the lead tank in a parade going into Jerusalem."[339] The Israelis treated Pollard

---

[334] Ibid., 36.

[335] Ibid., 144.

[336] Ibid., 166.

[337] Ibid., 175.

[338] Ibid., 177–178.

[339] Ibid., 208.

like a hero and in return he provided classified information. His ego was bolstered when he was told, "You're one of us."[340]

2. Addiction

Pollard admitted he used marijuana and cocaine on several occasions in the winter between 1982 and 1983.[341]

3. Ideology/Disillusionment/Loyalty

Pollard said he gave classified documents for ideological reasons, to help Israel, rather than for money. He did not believe his actions constituted disloyalty, although he did consider them dishonest.[342] Sarbin, Carney, and Eoyang speculate, "He seemed to be acting out of a sense of self-justification, against a background of what [he] considered to be a corrupt and morally defeated nation."[343] Pollard holds a theory there are

> three classes of Jews: those who travel to the holy land one or more times a year; those who don't or can't travel there but give Israel money and moral support; and finally, Jews like me who can't afford to travel to Israel or give money. When asked to help, we're willing to do anything for the love of our country.[344]

In a 61-page motion submitted by the defense prior to sentencing, Pollard stated his reason for spying "was to save Israel and to hurt the Soviet Union…[he] was motivated by anti-Semitism in his office…and would commit espionage for Israel again if given the chance."[345]

Pollard was later questioned under polygraph whether he had spied for Israel for financial gain and if he had lied about his true reason for spying. His answer did not indicate deception. He insisted initially it was for ideological reasons; however, Pollard

---

[340] Ibid., 64.

[341] Ibid., 34.

[342] Ibid., 208.

[343] Sarbin, Carney, and Eoyang, *Citizen Espionage*, 158.

[344] Olive, *Capturing Jonathan Pollard*, 182.

[345] Ibid., 61.

later admitted "he was corrupted by remuneration; he had developed an addiction to money."[346]

4. Security Concerns

Pollard had a history of embellishing or making up stories about his past. For example, in 1979, he told a colleague that his father had been the CIA station chief at the American embassy in South Africa and that he had contacts with the South African government,[347] which was false. During a security clearance background interview,

> Pollard claimed to have applied for a commission to become an officer in the Navy Reserve. He was a natural prevaricator in that he misrepresented his educational accomplishments, overstated his language ability, failed to mention his history of drug use, and again, lied about his father's relationship with the CIA.[348]

While working at the Naval Intelligence Support Center (NISC), Pollard worked long hours and weekends, often alone in a sensitive compartmented information facility. This should have been cause for concern, but no one reported the suspicious behavior.[349]

5. Financial Concerns

By the 1980s, "Pollard was starting to have problems with money. It was common knowledge that he had credit card debts, loan debts, debts on rent and incidental items. He missed his rent payment on December 1, 1983."[350] While co-workers were aware of his financial difficulty, no one reported anything. In 1984, Pollard received a letter of indebtedness from the Navy Federal Credit Union for three months of missed payment on a personal loan and a line of credit loan. As Olive explains:

> The navy personnel office forwarded the letter from the credit union to the NISC with a reminder that the employee should be informed of the navy's

---

[346] Ibid., 209.

[347] Ibid., 10.

[348] Ibid., 11.

[349] Ibid., 37.

[350] Ibid., 36.

> policy concerning indebtedness and that failure to pay a just debt may result in adverse action.[351]

This could have allowed for revocation of Pollard's clearance. As for long-term goals, aside from immediate payment for classified information, Pollard acknowledged that he hoped to go into preplanned business ventures when he left his position with the Navy.[352]

6. Childhood Upbringing

Pollard has been described as a social outcast, "a wise guy and a troublemaker, a flamboyant, loose-lipped person who invited insults and basked in attention, whether positive or negative."[353] He felt he was discriminated against because he was Jewish. An avid reader, he was considered a sissy when he was young and was bullied. He attended a private Jewish school. Olive notes, "There he flourished; playing the cello and reading every book he could lay his hands on."[354]

As a world renowned microbiologist, Pollard's father traveled extensively overseas giving lectures and attending conferences.[355] In his early teens, Pollard and his family traveled to Germany and toured the Dachau concentration camp. As Olive notes, "The experience shocked him, kindling a deep, enduring loyalty to Israel and the Jewish People."[356]

K. EDWARD SNOWDEN

Edward Snowden, a former intelligence contractor with the National Security Agency and the Central Intelligence Agency, disclosed details of classified U.S. and British mass surveillance programs that according to administration officials were used to detect and track suspected terrorist activity.[357] This breach of security caused extreme

---

[351] Ibid., 61.

[352] Ibid., 44–45.

[353] Ibid., 2.

[354] Ibid.,8.

[355] Ibid., 10.

[356] Ibid., 8.

[357] "Brazil Admits Spying of Foreign Diplomatic Targets," *Voice of America News*, November 4, 2013, http://www.voanews.com/content/brazil-admits-spying-on-foreign-diplomatic-targets/1783554.html.

damage to U.S.-foreign relations and is considered the most damaging leak in U.S. history. Much public debate has occurred over whether Snowden is a whistleblower, a traitor, or a patriot, and the incident has also sparked debate regarding government secrecy and openness. In June 2013, the U.S. Department of Justice charged Snowden with theft of government property, unauthorized communication of national defense information, and "willful communication of classified communications intelligence information to an unauthorized person,"— the last two charges were brought under the 1917 Espionage Act.[358] After fleeing to Hong Kong, Snowden was granted asylum by Russia where he remains a fugitive today.

1. Ego and Intellect

Snowden described himself as "a senior member of the intelligence community" when in fact he was a junior infrastructure analyst.[359] Greenwald, *The Guardian* newspaper columnist who first published the mass surveillance program information, found Snowden

> highly intelligent and rational, and his thought processes methodical. His answers were crisp, clear and cogent. In virtually every case, they were directly responsive to what I had asked, thoughtful and deliberate. There were no strange detours or wildly improbable stories of the type that are the hallmark of emotionally unstable people or those suffering from psychological afflictions. His stability and focus instilled confidence.[360]

Like many Americans, Snowden became more patriotic after the September 11, 2001 terrorist attacks. In 2004, at age 20, Snowden "enlisted in the U.S. Army intending to fight in the Iraq War, which he thought at the time was a noble effort to free the Iraqi people from oppression."[361] During basic training, he felt there was more talk of killing rather than liberating Iraqis. In a training accident, he broke both his legs, which ended

---

[358] Peter Finn, and Sari Horwitz, "U.S, Charges Snowden with Espionage, *Washington Post*, June 21, 2013, http://www.washingtonpost.com/world/national-security/us-charges-snowden-with-espionage/2013/06/21/507497d8-dab1-11e2-a016-92547bf094cc_story.html

[359] Harding, *The Snowden Files*, 71.

[360] Greenwald, *No Place to Hide*, 40.

[361] Ibid., 40–41.

his military career. Still wanting to serve the country, Snowden began his work with the federal government at the CIA.

2. Ideology/Disillusionment/Loyalty

As a result of the information to which he was privy:

> Snowden believed that the U.S. government's stealth attack on [the Constitution] was the equivalent of an attack that occupies land—a terrible and illegitimate invasion. He viewed his own deeds in explicitly patriotic terms. He saw his leak not as an act of betrayal but as a necessary corrective to a spy system that had grown dysfunctional.[362]

After fleeing to Russia and hoping to regain a more normal life in Germany, Snowden prepared a letter for a prominent member of Germany's Green Party, in which he states it was a moral duty which made him disclose the U.S. classified information.[363]

Rusbridger, the editor-in-chief of *The Guardian* newspaper opines,

> His motives are remarkable. Snowden set out to expose the true behavior of the U.S. National Security Agency and its allies. On present evidence, he has no interest in money—although he could have sold his documents to foreign intelligence services for many, many millions. Nor does he have the kind of left-wing or Marxist sentiments which could lead him to being depicted as un-American. On the contrary, he is an enthusiast for the American constitution, and, like other fellow "hacktivists," is a devotee of libertarian politician Ron Paul, whose views are well to the right of many Republicans.[364]

The countries that Snowden fled to (first to China, then to Russia) are known to violate human rights, limit personal freedoms, and to be places where free speech is repressed.

Snowden felt it was his obligation to the American people and other nations to disclose the information for humanitarian reasons. In his own words, "You realize that that's the world you helped create and it's gonna get worse with the next generation and

---

362 Harding, *The Snowden Files*, 110–111.

363 Romesh Ratnesar, "The Unbearable Narcissism of Edward Snowden," *Bloomberg Businessweek*, November 1, 2013, http://www.bloomberg.com/bw/articles/2013-11-01/the-unbearable-narcissism-of-edward-snowden

364 Harding, *The Snowden Files*, 1.

next generation who extend the capabilities of this sort of architecture of oppression."[365] He also declared,

> I want to spark a worldwide debate about privacy, Internet freedom, and the dangers of state surveillance. I'm not afraid of what will happen to me. I've accepted that my life will likely be over from my doing this. I am at peace with that. I know it's the right thing to do.[366]

He explains:

> Accordingly, I did what I believed right and began a campaign to correct this wrongdoing. I did not seek to enrich myself. I did not seek to sell U.S. secrets. I did not partner with any foreign governments to guarantee my safety. Instead, I took what I knew to the public, so what affects all of us can be discussed by all of us in the light of day, and I asked the world for justice. The moral decision to tell the public about spying that affects all of us has been costly, but it was the right thing to do and I have no regrets.[367]

3. Security Concerns

While working as a contractor at Booz, Allen, Hamilton, Snowden was fired "for violations of the firm's code of ethics."[368]

L. DEPARTMENT OF HOMELAND SECURITY CASES

The Department of Homeland Security (DHS) has two components in the Intelligence Community, DHS Headquarters (HQ) and the United States Coast Guard (USCG). The headquarters element, Intelligence and Analysis, is a consumer of other agencies intelligence, but it does not originate information. To date, there has been no DHS employee convicted of espionage. DHS was created with the passage of the Homeland Security Act in November 2002, which combined 22 different federal agencies and departments and officially standing alone on March 1, 2003.[369] Providing that some

---

365 Ibid., 149.

366 Greenwald, *No Place to Hide*, 18.

367 Harding, *The Snowden Files*, 238.

368 John Bacon, "Booz Allen says Edward Snowden was Fired for "Violation of the Firm's Code of Ethics." *USA Today*, June 11, 2013, http://www.usatoday.com/story/news/nation/2013/06/11/booz-allen-snowden-fired/2411231/

369 U.S. Department of Homeland Security, "Creation of the Department of Homeland Security," October 21, 2014, http://www.dhs.gov/creation-department-homeland-security

of the original employees continue to work at the department, it is feasible DHS could experience a serious event of unauthorized disclosure.

Research conducted by the Intelligence and National Security Alliance (INSA) has determined those who execute unauthorized disclosures do so after an average of 12 years of service.[370] This reflects the average time it takes for an employee to know a position well enough, have access to materials and achieve the comfort level to steal classified national security information and have the nerve to sell it or disclose it to the general public. There have, however, been releases of classified information to the media. In one case, a senior DHS official disclosed classified information to the media in order to promote a policy he supported. Once discovered, DHS opened an investigation; however, the employee left government service before remedial action could be taken. The Department of Justice declined to prosecute criminally. Without additional details, "ideology to promote policy" appears to be the primary indicator.

In another instance, a mid-level DHS employee disclosed classified information in a master's thesis while attending the Naval Postgraduate School. While classified, the information was identified from open-sources and was originally incorrectly marked by the originating agency. Portions of the thesis were later published in a scholarly journal, and an employee at the originating agency determined the information was classified. Investigation determined this to be a case of inadvertent disclosure, and no administrative action was taken.

The USCG is both an originator of sensitive maritime information and consumer of other agencies' intelligence. In a recent case, an intelligence specialist with the USCG admitted to passing classified material to foreign nationals and unauthorized individuals. He pleaded guilty in May 2012 to willful dereliction of duty to protect classified information.

From the research, the indicators of behavioral indicators of spying are ranked in the following order: ideology/disillusionment/loyalty concerns, large ego and high intellect, financial concerns and childhood upbringing, security concerns, and addiction.

370 Intelligence and National Security Alliance, *Leveraging Emerging Technologies*, 4.

VIII. DISCUSSION OF DATA

Upon review of existing data (see Table 1), the prevalent behavioral characteristic of the cases (10 out of 11 cases) is one of a disgruntled employee (*ideology/ disillusionment/loyalty*). A disgruntled employee becomes the largest concern of insider threat, one who is willing to compromise his or her feelings of loyalty to the organization and choose loyalty to oneself over country and colleagues. The Defense Personnel Security Research Center (PERSEREC) has noted in its studies, that since 1990 the majority of offenders are naturalized citizens.[371] This thesis research was based solely on native borne American citizens; however, it could easily be argued that in each case the individual had foreign connections, attachments, or ties. Most notable is the case of Ana Montes, who came from a Hispanic background and found herself disillusioned with U.S foreign policy toward Cuba. Divided loyalties can also be seen in the cases of Ames, Hanssen, and Walker, with their fascination with the Soviet Union and Russia. Manning and Snowden also felt foreign policy was misrepresented by U.S. presence in the Middle East. Pollard had feelings of discrimination because of his Jewish background.

The second predominant characteristic is *ego and intellect* (eight out of 10 cases). It could certainly be argued that in any of the cases studied, the individuals needed to be of some level of higher intelligence to be able to successfully remove classified national security information from their places of employment, transmit it to an outside source, or take it from the confines of the workplace and drop it at designated locations. Certainly in the cases of Ames, Montes, Hanssen, Walker, and Pollard, the longevity of their careers in spying reflects a certain level of skill and cunning. Interestingly, a number of the

[371] According to Herbig: "While before 1990, roughly 80% of American spies were native-born citizens, since 1990 the percentage of native-born offenders has fallen to 65%, while the corresponding percentage of naturalized citizens rose to 35%. Also since 1990, the percentage of American spies with foreign attachments (relatives or close friends overseas) increased to 58% and those with foreign business or professional connections jumped to 50%. From less than 10% before 1990 who had cultural ties to foreign countries, that percentage with foreign cultural ties increased to 50%. Divided loyalties, defined here as holding and acting on an allegiance to a foreign country or cause in addition to or in preference to allegiance to the United States, increased dramatically since 1990. Compared to the two earlier periods, in which divided loyalties were the sole motive for espionage by less than 20%, since 1990, 57% of Americans were motivated solely by divided loyalties." Herbig, *Changes in Espionage by Americans: 1947–2007*.

people in the cases had personality quirks. Those with high intellect were able to persuade colleagues and supervisors of their innocence. Indeed, Ames was able to forge his own security clearance as well as pass polygraph exams—even while being deceptive. Fischer refers to a frequent trait of those who spy when he wrote: "obsessive self-centeredness or selfishness—a lack of genuine caring for others and an indifference to problems experienced by other persons."[372] This is clearly illustrated by the comments made by Montes's sister, when she wrote,

> You betrayed your family, you betrayed all your friends. Everyone who loves you was betrayed by you. You betrayed your co-workers and your employer, and you betrayed your nation. You worked for an evil megalomaniac who shares or sells our secrets to our enemies.[373]

Project Slammer, "an innovative community research program using…behavioral science techniques…to better understand and deter espionage,"[374] has concluded from psychological testing and interviews that those who commit espionage have "two, almost opposite, personality types among [the] 30 offenders under study—one, a highly manipulative, dominant and self-serving type; the other, passive, easily influenced and lacking self-esteem."[375]

Financial concern (seven out of 11 cases) is often thought to be a high motivator, notwithstanding PERSEREC's determination. Since 1990, 80 percent of those who committed unauthorized disclosure did so voluntarily and without payment.[376] Those who did receive payment included Ames, Hanssen, Pollard, and Walker who began selling information prior to the 1990s and were well compensated. In 2008, Bergersen was successfully paid and was certainly motivated by financial gain, as were Regan and Underwood. Later incidents indicate a possible shift in motivation for divulging state secrets. Montes, while beginning her spy career in 1985, did so primarily for ideological

---

372 Fischer, *Espionage: Why Does it Happen?*, 7.

373 Popkin, "Ana Montes Did Much Harm Spying for Cuba."

374 https://antipolygraph.org/documents/slammer-12-04-1990.shtml. Director of Central Intelligence Staff-Intelligence Community Staff. Memorandum for: Members, DCI Security Forum. Subject: *Project SLAMMER Interim Report.* Washington, DC. April 12, 1990.

375 Fischer, *Espionage: Why Does it Happen?*, 7.

376 Herbig, *Changes in Espionage by Americans: 1947–2007*.

reasons, as did Abu-Jihaad, Manning, and Snowden. This may indicate a shift in the way citizens view the U.S. government (i.e., a government that while declaring more transparency actually seems to exhibit more secrecy). Indeed, Sarbin, Carney, and Eoyang found that in reviewing

> case summaries of convicted citizen spies [from 1984–1994] shows that the most frequently mentioned reason for stealing and selling government secrets is financial gain. To a lesser extent, some offenders tell a story in which they perceive themselves as victims of unjust authority and construe their theft and marketing of secrets as revenge. In at least one case, the theft and attempted sale of information was in part motivated by 'sensation seeking,' the feeling of excitement that frequently accompanies the commission of a forbidden act. Save for the few offenders whose motives stemmed from political convictions, financial gain appeared to be a significant element in the motive structure of known spies.[377]

Sibley goes beyond financial gain, expressing:

> We tend to think people are largely motivated by material concerns. But that's superficial. We're also motivated by what the philosophers call the desire for recognition. Beyond food, shelter, sex and comfort, we much more powerfully seek to establish our lives as significant and meaningful.[378]

Thus, he notes about Hanssen:

> Seen this way, money was icing on the cake for Hanssen. More telling is his apparent disdain for his country. America, [Hanssen] wrote, "can be errantly likened to a powerfully built, but retarded child, potentially dangerous, but young, immature and easily manipulated." This not only suggests someone alienated from society, but, conversely, someone frustrated by society's lack of recognition.[379]

While personal security background investigations review information from the present as far back as 10 years prior, studies of espionage based on personal interviews with offenders suggest a pattern in which personal disruptions or crises precede, or 'trigger,' an individual's decision to commit espionage. Crises could be positive or

---

377 Sarbin, Carney, and Eoyang, *Citizen Espionage*, 111.

378 Robert Sibley, "The New Spy Game: For Robert Hanssen, It Appeared to be More about a Desire for Recognition than Greed," *The Halifax Daily News*, February 27, 2001, 20.

379 Ibid., 20.

negative, and include divorce, death, starting a new relationship, or observed by exhibiting radically changed behavior. Commentators have speculated that if help or timely intervention had been offered in these cases, the crime might have been averted.[380]

Thus,

> Assessing the quality of a person's moral development at an early life stage may be irrelevant to the context of later action when unforeseen events create a condition of personal strain for which trust violation would be a possible resolution.[381]

These stressors may be better understood using the context of Henri Tajfel's social identity theory (SIT). Tajfel explains: "Social identity is understood as the part of the individuals' self-concept which derives from knowledge of their membership of a social group (or groups) together with the value and emotional significance attached to that membership."[382] What leads some to leave social groups, co-workers, and the organization, in search of other groups (i.e., foreign countries)? Examination of the various cases using SIT may provide some insight as to not only why, by how authorities could have detected basic changes in a person's character. Ames diagnosis himself using SIT. He explains:

> My frustration comes from attempts by you [the author of Ames' story, Peter Earley] and my FBI and CIA debriefers to simplify and find a single, overriding reason for what happened, when, in fact, there is no single reason, but layers upon layers upon layers of reasons, none more pressing than the others, and added to these layers are the events themselves, an almost-never-to-be-repeated coming together of circumstances, which facilitated a fantasy, causing it suddenly to gel, without conscious realization or careful, even painful, thought, into a real plan…. The unique circumstances were critical. They created the opportunity…. To attempt to rank or segregate or declare that one factor provides the explanation is to deny how a person feels, thinks, and acts.[383]

---

380 Herbig, *Changes in Espionage by Americans: 1947–2007*, xi.

381 Sarbin, Carney, and Eoyang, *Citizen Espionage*, 119.

382 Henri Tajfel, *Social Identity and Intergroup Relations* (Cambridge: Cambridge University Press, 1982), 2.

383 Earley, *Confessions of a Spy*, 348–349.

It can be argued almost every individual experiences some suffering during childhood (*childhood concerns*), whether abuse by family members, classmates, or bullies (as did individuals in seven out of 11 cases). However, when reviewing the numbers of known unauthorized disclosures in relation to the half million or more U.S. personal security clearance holders, most will not sell or give classified national security information away. Sarbin, Carney and Eoyang believe spying is strongly related to:

> A common…contributing condition is the experience of alienation, of low self-esteem, a condition for which money is often seen as a solution. When lawful means of dealing with self-esteem problems are in short supply or exhausted, the potential offender may consider illegitimate means….ready to incorporate the plot of spy into his self-narrative.[384]

Fischer notes, "We do know…many were victims of severe child abuse which resulted in an intense self-esteem problem. Others appear to have been raised without the benefit of moral training or positive role models."[385] For example, Ames was encouraged to learn about the finer things in life when he was young and told he was better than others. In other examples, Hanssen and Walker were psychologically and physically abused, and Manning believes her father ejected her from his residence as a result of her sexual orientation. Whether physical or emotional, if an individual does not have the coping skills and is psychologically vulnerable, additional stressors most likely will result in impairment of the individual's judgement.

In six out of the 11 cases reviewed, individuals had histories of serious *security concerns* prior to apprehension (except in the case of Edward Snowden who remains on temporary asylum in Russia). While security violations of several of the individuals were noted within their organizations, they were rarely admonished. For example, even if a recommendation was made to downgrade or suspend a security clearance of an individual, often no further action would be taken at the next level or the individual would change positions in order to avoid revocation of clearances. Ames and Walker were noted for foreign contact and alcoholism. They, along with Hanssen, were noted for their affluence. Yet, because of personality traits, colleagues wanted to believe there was

---

[384] Sarbin, Carney, and Eoyang, *Citizen Espionage*, 124.

[385] Fischer, *Espionage: Why Does it Happen?*, 8.

nothing amiss. This, in part, is an aspect of the office culture that must change. Co-workers must feel empowered and supported in informing supervisors or security personnel of behavioral and character changes that create security concerns.

Manning was reprimanded for releasing sensitive information in a YouTube post, two years before her unauthorized disclosure to Wikileaks. She had a history of aggressive behavior towards fellow soldiers, as well as dealing with the psychological pressure of being a homosexual or transgender in the era of the military's don't ask, don't tell policy. Meanwhile, Snowden was fired for violating his workplace ethics code. If security concerns were taken more seriously, many unauthorized disclosures could have been mitigated or prevented.

Finally, *addiction* to alcohol or drugs was documented in only four of the 11 cases I studied. In the case of Hanssen, I have characterized a sex addiction. Additionally, it could be argued that all of the cases exhibit some sort of addiction. Perhaps in a broader sense, addiction could be related to the exhilaration of being a spy, being perceived as a patriot, or changing foreign policy. However, in 2014, Paul Johnson found that a significant number of those who were determined to be insider threats have an addiction to gambling or prescription drugs and that financing these addictions is a primary motivator for associated criminal behavior.[386]

[386] Paul R. Johnson, "Trusted Insiders are Committing Fraud and Embezzlement within Organizations: Is there a Connection to Addiction, as the Motivating Factor for their Illegal Activities?" (master's thesis, Naval Postgraduate School, 2014), 5–6.

Table 1. Behavioral Indicators Found in Cases Reviewed

Subject Characteristic	Ego and Intellect	Addiction	Ideology/ Disillusionment/ Loyalty	Security Concerns	Financial Concerns	Childhood Upbringing
Ames	X	X	X	X	X	
Montes	X		X			X
Manning	X		X	X		X
Regan	X		X		X	X
Underwood					X	X
Bergersen			X		X	
Abu-Jihaad			X			
Hanssen	X	X	X	X	X	X
Walker	X	X	X	X	X	X
Pollard	X	X	X	X	X	X
Snowden	X		X	X		
TOTAL	8	4	10	6	7	7

In the final analysis, there is no way to determine how many potential spies or persons bent on disclosing classified information have been eliminated through the vetting of data collected during the initial security clearance request process. Depicted in this thesis is the result of employees who passed the screening process and were fully trusted in performing their duties. The conclusion to be drawn from this is two-fold. First, first- and second-line managers of employees who have access to classified information must be keenly aware of any changes in the personality of their employees. They must go beyond simply giving work assignments and grading results. In addition, managers have to be able to read slight changes in attitude, performance, personality, and be prepared to make tough decisions about taking positive action when nuances, however slight, are detected. Because intellect and ego play an important part in employee performance, managers must be trained to deal with employees whose behavior is outside the norm in those regards. Second, managers must, on a regular basis, encourage all employees to be mindful of personality or lifestyle changes of fellow employees and provide a protected avenue for them to discuss fellow employee behavior. “See something, say something” is a phrase that belongs in the work place and applies to both personality and material things. Recognizing and dealing with disgruntled employees might just prevent or mitigate unauthorized disclosure. Disgruntlement leads to changes in ideology, disillusionment with one’s organization, and ultimately may change a person’s national loyalty; these are the predominant factors found supervisors must be aware of.

IX. CONCLUSIONS AND RECOMMENDATIONS

Conclusion 1

Unauthorized disclosure of classified information can have many results: compromise of intelligence sources and collection methods, loss of life, financial impact, and serious harmful effects on U.S. foreign relations. This research has found that ideology, disillusionment, and questionable loyalty are primary motivators for a person to release classified information without authorization. Disclosures are often related to personal crises, such as financial problems, some type of addiction, or divorce. However, millions of federal employees with access to classified information face similar personal crises in their lives; yet, they do not commit unauthorized disclosure. According to Herbig:

> Pressure does tip some people away from their apparent stability into doing impulsive or desperate things, and espionage is occasionally one of those desperate things. At a minimum, this suggests that managers of employees with access to classified or sensitive information **should** take seriously their responsibility to be aware of unusual stresses in their employees' lives, and to sensitively monitor and try to assist employees in crisis.[387]

People change over time as they face many difficult life events.

Recommendation 1

Management must continually monitor employee behavior to ensure employees remain reliable, trustworthy, of good conduct and character, and loyal to the United States throughout their time of employment and into post-employment. This is especially critical for first- and second-line supervisors. In the military, there are many stories about first-line supervisors (squad leaders) and second-line supervisors (platoon sergeants and platoon leaders) who are intimately involved in their "employees" lives and are well aware of what is happening in their lives on and off the job. It is not as easy in the civilian world, but civilian supervisors must have a feel for what is going on in the lives

[387] Herbig, *Changes in Espionage by Americans: 1947–2007*, 43–44.

of their employees. This can occur as simply as organizing periodic in-office social functions such as birthday observances, occasional office potluck lunches, and recognition and awards ceremonies. Semi-annual or annual evening functions are another option. It is important supervisors use each of these occasions to talk with their employees to genuinely determine employee satisfaction or dissatisfaction and any changes that might be occurring in their lives.

Conclusion 2

Increased, in-depth background investigations and vetting **would** enhance the prevention of unauthorized disclosure. Currently, initial and subsequent investigations are incomplete or inaccurate because potential or active clearance holders fail to report past or current offenses, use false identities, or are born and raised in foreign countries where records may be difficult to review. In addition, inaccurate or incomplete reports are often a result of one agency failing to provide information to another for a variety of reasons. Thirty years ago, Jonathan Pollard applied for a position with the Central Intelligence Agency but was rejected for admitting extensive drug use. Upon applying to the Navy, the Navy requested any information about Pollard from the CIA. The CIA denied such information believing Pollard had a right to privacy.[388] This simple exchange of information could have prevented Pollard from obtaining a clearance and going on to sell classified information.

Recommendation 2

DHS HQ must engage Congress to enact legislation that directs all federal agencies to respond accurately and in a timely manner to all requests for information from the Central Clearance Facility (CCF) in support of a background investigation on a prospective federal clearance holder. The CCF must work with each state to obtain similar transparency so state criminal and financial data bases can be queried by CCF.

388 Olive, *Capturing Jonathan Pollard*, 9–10.

Conclusion 3

Self-reporting changes in lifestyles (positive or negative) are a critical piece in maintaining employee accountability for being a trusted person. Fear of repercussion is a major factor in employees' not self-reporting drastic changes. According to Chaney, "The true cases of concern are those individuals who can preserve a calm outward demeanor while their private life descends into an awful pit."[389] Intelligence community professionals recognize that revealing negative life events can result in discipline, which can include revocation of a clearance and possibly dismissal from government service. Chaney views the insider threat as an individual who has problems coping with stress. He explains:

> The insider spy seriously considers himself to be a patriotic American. Old-fashioned traditional values that were imbued in him in grade school stay alive within his heart. The insider spy's beef was usually never with our country. His beef was really with himself. At his weakest moment, his way of handling overwhelming stress was to project his self-disappointment and anger onto the nearest handy target, typically his home agency.[390]

Also it is paramount for co-workers and supervisors to notice changes in employee activities, and they **must** be empowered to report suspicious behavior. Colleagues do not want to think the worst about those with whom they work, let alone report those suspicions to management; however, sometimes this is exactly what **must** be done. Early intervention to prevent an employee going by the wayside **could** help prevent unauthorized disclosures.

Recommendation 3

Managers must implement training programs that extol the benefits of self-reporting and assure employees there are programs to help them get through any current problems that could make them a security risk. If the employee completes the program, it is possible that the employee can be returned to full employment or placed in a non-classified position.

---

389 Chaney, *Noir: A White Paper*, 8.

390 Ibid., 15.

Conclusion 4

Executive Order 13589, Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information, was issued in 2011; however, in January 2015, DOD reported its Insider Threat Detection Program estimated initial operating capability is not expected until January 2017 with no projection when full operating capability will occur.[391] This executive action is a direct result of the WikiLeaks disclosures. The executive order requires the federal government, under the co-chair of the director of national intelligence and the attorney general, to develop an insider threat program for:

> deterring, detecting, and mitigating insider threats, including the safeguarding of classified information from exploitation, compromise, or other unauthorized disclosure, taking into account risk levels, as well as the distinct needs, missions, and systems of individual agencies. This program shall include development of policies, objectives, and priorities for establishing and integrating security, counterintelligence, user audits and monitoring, and other safeguarding capabilities and practices within agencies.[392]

Recommendation 4

DHS HQ **must** determine what assistance is required to develop an insider threat program to allow for earlier implementation. This will require direct coordination with the offices working this issue at the national level.

Conclusion 5

The current security clearance process is weak and needs to be revamped. As Sarbin, Carney, and Eoyang illustrate, there is no method that could identify current or future "spies" and differentiate them from innocent employees. They continue to say, "The issue becomes especially controversial when it comes to assessments of personal loyalty, patriotism and reliability."[393] This certainly can be seen in the cases of Chelsea

---

391 Steven Aftergood, "Insider Threat" Program Lags behind Schedule," Federation of American Scientists, January 12, 2015, http://fas.org/blogs/secrecy/2015/01/insider-threat-lags/

392 Exec. Order No. 13587, 76 Fed. Reg. 198 (October 13, 2011), §6.1

393 Sarbin, Carney, and Eoyang, *Citizen Espionage*, 70.

Manning and Edward Snowden. Public opinion is widely divided whether these two are traitors or heroes. Known unauthorized disclosure instances are rare:

> each known case very complex, and scientific research virtually nonexistent, there is no well-established characteristic, psychological or otherwise, that can serve as a reliable indicator of spying propensity…. While all spies may be dishonest, very few dishonest individuals are spies.[394]

If clearance processes were so stringent to detect individuals who may disclose information, many innocent personnel could also be determined to be security risks.

The Defense Security Service (DSS) notes that background investigations are missing critical information such as self-reported character flaws or misbehavior and information contained in state and local criminal records. While current law requires this information to be provided to an investigator, no action is taken against those states and localities that do not comply.[395] This results in incomplete investigations that pave the way for favorable adjudications and granting of security clearances that might otherwise not have been granted. This happened in the case of Aaron Alexis, the Washington Navy Yard shooter. While this was not a "disclosure" incident, Alexis was able to gain access to a restricted area by virtue of his security clearance.

Recommendation 5

A commission led by the Office of Personnel Management should be formed to look at improving security clearance processes. Additionally, there **must** be strict enforcement of laws that grant clearance processors authority to access state and local records.

Conclusion 6

Peer reporting rarely occurs. Personnel **must** understand and feel confident in reporting requirements of suspicious behaviors or life-changing events affecting their colleagues. This includes, but is not limited to, intention to marry a foreign national,

394 Ibid., 73–74.

395 Defense Security Service, *Roles and Responsibilities for Personnel Security*, 5–6.

unusual and frequent foreign travel, bankruptcy, or treatment for drug and alcohol abuse. The potential of having an employee who might disclose classified information can be reduced if colleagues are able to recognize the potential indicators and are willing to intervene.[396] An individual lacking the coping mechanisms or the support system to deal with stressful life events may become susceptible to committing unauthorized disclosures. The organization and its personnel **must** make a commitment to uphold social conventions and intervene early when behavioral indicators show an employee may become susceptible to committing a crime. Important factors in instilling organization culture are "group cohesiveness, group incentive (reward) structures, relatively small group size, membership stability and relatively high functional dependence among group members."[397] While the federal government, as a whole, is certainly not a small group size, those teams who share projects and view the same classified information are. These small groups **must** unify to establish the overall organizational culture, one to which each employee is bonded. According to a report by PERSEREC,

> Under internal control systems, the group uses its social influence to regulate members' work activities. Identification with and loyalty to one's colleagues are thought to be engendered when a group member sees himself or herself as a pivotal contributor to the group's outcomes and when the group is viewed by the member to be to be an important source of personal successes. Internal control systems encourage such states by emphasizing personal responsibility to one's colleagues, and adherence to the work group's standards for conduct.[398]

Recommendation 6

The executive branch should amend E.O. 13589 and add mandatory training for all employees and supervisors as a part of each federal agency's insider threat program. This will strengthen and mandate training in peer reporting for both employees and enhance supervisors' abilities to handle such reports. A part of this program must ensure

396 Defense Personnel Security Research Center *Espionage and Other Compromises of National Security*, iii.

397 Sarbin, Carney, and Eoyang, *Citizen Espionage*, 172.

398 Ibid., 173.

employees are granted complete privacy and anonymity when reporting on a fellow employee's changed behavior or significant lifestyle changes.

Conclusion 7

Until this year, there has been no systematic method to continuously evaluate employee behavior or character changes. E.O. 13467 defines continuous evaluation (CE) as:

> reviewing the background of an individual who has been determined to be eligible for access to classified information (including additional or new checks of commercial databases, government databases, and other information lawfully available to security officials) at any time during the period of eligibility to determine whether that individual continues to meet the requirements for eligibility for access to classified information.[399]

Assessing data automatically derived from credit background checks, social media, personnel records, and self-reporting records, may reveal relevant information, prompting further investigation and enabling agencies to prioritize their efforts on those who appear to have the highest risk. As noted earlier, there are many inaccuracies in obtaining data in the initial clearance process. This could be critical information in granting or not granting a clearance. Recently, the Department of Defense initiated a pilot program that tested the validity of its Automated Continuous Evaluation System (ACES). The test program sampled 3,370 Army service members, civilian employees, and contractor personnel. It discovered that 21.7 percent of the tested population had previously unreported derogatory information that had developed since the last investigation, and three percent had serious derogatory information (for example, financial issues, domestic abuse, drug abuse) that resulted in a revocation or suspension of a security clearance.[400] The frequency of these data checks **would** allow for a more real-time assessment to better monitor the behavior of any clearance holder and alert security officers for the need to

---

399 Exec. Order No. 13467.

400 Joe Davidson, "More Frequent Automated Security Clearance Checks Likely in Defense and Other Agencies," *The Federal Diary*, March 25, 2013, http://www.washingtonpost.com/politics/federal_government/more-frequent-automated-security-clearance-checks-likely-in-defense-and-other-agencies/2014/03/25/6d313b80-b43e-11e3-b899-20667de76985_story.html

conduct an investigation. Using a program such as ACES could significantly reduce the cost of background investigations by monitoring employees in real time on a random and more frequent basis. However, there has to be an acceptable level of confidence in the ACES results to make it worthwhile.

Recommendation 7

> [That the] National Counterintelligence and Security Center (NCSC) in the Office of the Director of National Intelligence (ODNI) [aggressively continue to establish] a Continuous Evaluation Program (CEP) to develop an enterprise-wide CE tool for Executive Branch use, and to coordinate, align, and integrate Executive Branch departments and agencies' CE activities to address these conclusions…. A limited CE capability will be developed and implemented in select agencies for a portion of the [Top Secret]TS/SCI-cleared population in FY 2015, with the objective of expanding to all executive branch departments and agencies with a TS/SCI population by the end of FY 2016. Executive Branch departments and agencies will align and integrate their agency-specific CE capabilities to the new federal CE solution.[401]

Conclusion 8

There appears to be no consistent or continuous review of positions where classified documents are handled. According to a guide by the Defense Security Service:

> Executive branch policy expressly directs agencies to minimize the number of individuals with eligibility for access to classified information to that required to conduct agency functions. It also expressly prohibits requesting eligibility in excess of actual requirements. Despite these policies, 5.1 million employees and contractors were eligible for security clearances as of October 2013.[402]

Many positions may no longer require access to classified information or could be downgraded to a lower security clearance level, resulting in decreased costs of maintaining a security clearance with reduced periodic reinvestigations or eliminating the

---

401 National Counterintelligence and Security Center, *Continuous Evaluation Program Fact Sheet*, http://www.ncsc.gov/SEA/docs/Continuous_Evaluation_Fact_Sheet.pdf

402 White House, *Suitability and Security Processes Review: Report to the President*, 2014, https://www.whitehouse.gov/sites/default/files/omb/reports/suitability-and-security-process-review-report.pdf, 12.

requirement for a clearance. This thought is echoed by the Committee on Oversight and Government Reform, which writes:

> In 2012, 4.9 million Americans—over 1.5 percent of our country's population—held security clearances. The Executive Branch **must** study whether so many clearances are necessary, and find ways to better determine whether someone needs access to classified materials or spaces. The Executive Branch **should** take steps to reduce the over-classification of information, which **would** reduce the number of clearances needed. Another possible solution is to create a system of temporary clearances that expire after a pre-determined amount of time. Ensuring that only those who actually need security clearances receive clearances **would** go a long way to reducing the pressures on the investigation and adjudication processes.[403]

Recommendation 8

The secretary of homeland security must engage the director of national intelligence (DNI) to issue guidance to all executive agencies on determining what positions require security clearances. In addition, DNI must implement some method of ensuring periodic review of such positions to determine continued validity.

Conclusion 9

The Internet and social media sites along with traditional media venues have lessened the standard obstacles in disclosing classified information without authorization and have "dramatically increased the ease with which reporters, editors and publishers can evade laws or regulations pertaining to the publication [of] classified information."[404] Releasing classified information has become exceptionally simplified with the creation of disclosure websites such as WikiLeaks and Cryptome on which one can anonymously upload information to the site for broadcast to a wide population. Sarbin, Carney, and Eoyang note traditional media assists in promulgating the information pointing out "it is unlikely that WikiLeaks data dump **would** have had the public impact that it did, had *The New York Times* not curated the disclosures, drawing the attention of readers to particular

403 *Slipping Through the Cracks*, 13.

404 Sagar, *Secrets and Leaks*, 178.

facts, providing context, and commissioning supporting editorials."[405] Modern mass media and Internet access allowed disclosures by Chelsea Manning and Edward Snowden to broadcast American secrets throughout the United States and worldwide.

Recommendation 9

The Center for Security Clearances **must** explore new automated technologies, as well as media security technologies, in order to determine critical indicators that may shed light on character flaws of current and prospective government security clearance holders.

Conclusion 10

While the number of overall unauthorized disclosure cases is small, the information disclosed has been significant. As noted, the primary reasons for unauthorized disclosure found during this research are ideology, disillusionment, and loyalty. As such, the most effective approach to prevent unauthorized disclosure is to create a work environment that provides for high morale, and loyalty to the organization and co-workers. According to Sarbin, Carney, and Eoyang, "Instilling organizational pride, promoting esprit de corps, and making someone a winning team are all means to stimulate positive effects."[406] Organizations **must** "create opportunities to deal with disgruntled employees, employees with financial problems, or employees with alcohol or drug dependencies before they took revenge or betrayed their trust by disclosing classified information or selling trade secrets."[407] Disgruntled employees **must** have an outlet to address their grievances. There was no such venue in the cases of Aldrich Ames and Robert Hanssen. Once Ana Montes made her feelings against U.S. foreign policy clear, access to classified information **should** have been limited immediately. Sarbin, Carney, and Eoyang argue, "More powerful prevention and detection results could be obtained by relying on the promotion of strong group cohesiveness coupled with social

405 Ibid., 178–179.

406 Sarbin, Carney, and Eoyang, *Citizen Espionage*, 8.

407 Ibid., 14.

integrity that enforces responsibility for security on those closest to the problems."[408] Cohesiveness is enforced by a culture of social control. Sarbin, Carney, and Eoyang explain:

> The essential elements are 1) the individual; 2) a social entity—not just the generalized society but a defined social entity such as a family, a tribe, a school, a military unit, or a psychological researcher; and 3) some kind of co-presence, so that the individual is with the social entity, at least in a psychological sense but usually in an obvious physical sense. Social control in operation is pervasive and simple: The individual acts in conformity to the norms, values and standards of the salient social entity. This is normatively what happens all the time. We are conforming, we are obedient, and we observe and respect social conventions. We are largely—all of us—under social control most of the time.[409]

Recommendation 10

Managers (supervisors) and fellow employees must be vigilant and question any situation where any one individual amasses a significant amount of classified information or stores a massive amount on a computer or external hard drive. Constant monitoring of stored classified information should be mandatory. In the past, as well as in the current climate, employees are allowed to store metadata on computers without those files being logged in/logged out or accounted for. This recommendation will indeed demand a change in the way the government accounts for stored electronic files.

Conclusion 11

A person's untrustworthiness is difficult to assess or measure using current methodology.

Recommendation 11

A wide variety of personality tests have been developed, notably the Myers Briggs Type Indicator (MBTI), the MMPI, and a number of tests based on the five factor model of personality, such as the Revised NEO Personality Inventory.[410] Short of a

---

[408] Ibid., 90.

[409] Ibid., 154.

[410] *Wikipedia*, "Personality Test," accessed May 2, 2015, http://en.wikipedia.org/wiki/Personality_test

number of expensive psychiatric visits, administering personality tests could be an expensive yet effective method to initially determine if a person being considered for a security clearance in the federal government. The recommendation would include administering the tests during follow-up investigations or clearance renewal.

X. EPILOGUE

Ultimately, the insider threat is a person who works among us. Although the DHS has not suffered the expense and embarrassment of an insider divulging a serious volume of sensitive or classified information, it should take a very strong stance on implementing extensive training programs that target employees and supervisors. Its system must be strengthened using modern information technology employing current social behavior software. Additionally, colleagues and first line managers **must** be empowered to monitor, report, respond, and mitigate suspicious behavior to prevent unauthorized disclosure. Effective training and awareness programs **must** be fully developed. Employees **must** understand their roles and responsibilities, whether a security clearance holder or not. These training programs must not be ones that sit on the shelf only to be reviewed after an incident occurs, they must be developed, employed, and updated on a regular basis. At a minimum, insider threat awareness should be a mandatory, quarterly all personnel presentation. Studies by Fischer determined:

> Many…former spies claim that their decision to commit this crime was based in part on their belief that the probability of being noticed and reported by co-workers was next to nothing…. Intervene in the interest of an at-risk employee before he or she becomes a threat to national security. … A workplace in which people are known to be aware and willing to take action when appropriate presents a powerful deterrent to espionage.[411]

Without a diligent workforce that is trained to detect even minor character changes in colleagues, the ability to prevent unauthorized disclosure is greatly diminished. DHS must participate in a complete review of the security clearance process in coordination with other federal agencies. DHS should be the initiator in the formation of a joint federal agency commission that reviews the present security clearance process and recommends implementation of improved processes that enhance the security clearance program. Finally, DHS should complete a comprehensive review of all positions currently requiring a security clearance to ensure access to classified

411 Fischer, *Espionage: Why Does it Happen?*, 9.

information is limited to persons whose official duties require knowledge of possession of classified information.

LIST OF REFERENCES

Aftergood, Steven. “Insider Threat Program Lags behind Schedule.” Federation of American Scientists. January 12, 2015. http://fas.org/blogs/secrecy/2015/01/insider-threat-lags/

Alford, C. F., and Corrine Bendersky. “Whistleblowers: Broken Lives and Organization Power.” *Labour* no. 51 (spring 2003): 321–323.

Andress, Jamal. “Army Specialist Ivan Lopez: What We Know about the Fort Hood Shooter.” *ABC*, April 2, 2014. http://www.abc15.com/news/national/army-specialist-ivan-lopez-what-we-know-about-fort-hood-shooter

Apple, Jr., Raymond. W. “25 Years Later. Lessons Learned from the Pentagon Papers.” *The New York Times*, June 23, 1996. http://www.nytimes.com/1996/06/23/weekinreview/25-years-later-lessons-from-the-pentagon-papers.html

Bacon, John. “Booz Allen says Edward Snowden was Fired for “Violation of the Firm’s Code of Ethics.” *USA Today*, June 11, 2013. http://www.usatoday.com/story/news/nation/2013/06/11/booz-allen-snowden-fired/2411231/

Bauerle, James. “Golden Eye Redux.” *Banking Law Journal* 120, no. 3 (2003): 266–278.

Baumann, Paul. “Agent Hanssen: The Spy Who Came in from the Fold.” *Commonweal*, March 23, 2001.

Bhattacharjee, Yudhijit. “Hide and Seek.” *Wired* 18, no. 2 (February 2010). http://www.wired.com/2010/01/ff_hideandseek/

Blake, Aaron. “Americans: Snowden is a Whistleblower, not a Traitor. Numerous Members of Congress have Labeled Edward Snowden a Traitor, but the American People Aren’t On-board Yet.” *Washington Post*, July 12, 2013.

Blitzer, Wolf. “Pollard: Not a Bumbler, but Israel’s Master Spy.” *Washington Post*, February 15, 1987. http://www.jonathanpollard.org/7890/021587.htm

Bridis, Ted. “Defiant U.S. Intelligence Analyst Sentenced to 25 Years for Spying.” The Associated Press. October 17, 2002. http://www.freerepublic.com/focus/news/770647/posts

Brown, Anthony Cave, and Charles B. MacDonald, eds. *The Secret History of the Atomic Bomb*. New York: Dial Press, 1977.

Bunn, Matthew, Martin B. Malin, Nickolas Roth, and William H. Tobey *Project on Managing the Atom: Advancing Nuclear Security: Evaluating Progress and Setting New Goals*. Cambridge, MA: Harvard Kennedy School, Belfer Center for Science and International Affairs, 2014.

Bunn, Matthew, and Scott D. Sagan. *A Worst Practices Guide to Insider Threats: Lessons from Past Mistakes*. Cambridge: American Academy of Arts and Sciences, 2014. https://www.amacad.org/multimedia/pdfs/publications/researchpapersmonographs/insiderThreats.pdf

Burke, Cathy. "Report: DHS Employee Maintains Anti-White, Anti-Gay Site." *Newsmax*, May 21, 2015. http://www.newsmax.com/US/dhs-employee-anti-white/2013/08/22/id/521670/

Carmichael, Scott W. *True Believer: Inside the Investigation and Capture of Ana Montes, Cuba's Master Spy*. Annapolis, MD: Naval Institute Press, 2007.

"Chairman Carper, Ranking Member Coburn Continue Oversight in Wake of Navy Yard Shooting." U.S Senate Committee on Homeland Security and Governmental Affairs. September 19, 2013. http://www.hsgac.senate.gov/media/minority-media/chairman-carper-ranking-member-coburn-continue-oversight-in-wake-of-navy-yard-shooting

Chaney, David L. *Noir: A White Paper.* 2014. http://www.noir4usa.org/wp-content/uploads/2014/07/NOIR-White-Paper-17JUL14.pdf

Chapman, Suzann. "Retired Airman Faces Death Penalty in Espionage Case." *Air Force Magazine* 85, no. 6 (2002): 19.

Cherkashin, Victor, and Gregory Feifer. *Spy Handler: Memoir of a KGB Officer: The True Story of the Man Who Recruited Robert Hanssen and Aldrich Ames*. Cambridge: Basic Books, 2005.

Davidson, Joe. "More Frequent Automated Security Clearance Checks Likely in Defense and Other Agencies." *The Federal Diary*, March 25, 2013. http://www.washingtonpost.com/politics/federal_government/more-frequent-automated-security-clearance-checks-likely-in-defense-and-other-agencies/2014/03/25/6d313b80-b43e-11e3-b899-20667de76985_story.html

Defense Personnel Security Research Center. *Espionage and Other Compromises of National Security. Case Summaries from 1975 to 2008*. Monterey, CA: Defense Personnel Security Research Center, 2009.

———. *Insider Risk Evaluation and Audit Tool* (PP 09–03). August 2009. http://www.dhra.mil/perserec/reports/pp09-03.pdf

Defense Security Service. *Roles and Responsibilities for Personnel Security: A Guide for Supervisors*. Accessed June 2, 2014. http://www.cdse.edu/documents/cdse/Supv_Role_in_PerSec.pdf

———. *So You Need a Security Clearance: How to Receive and Maintain Your Security Clearance*. Washington, DC: Defense Security Service. http://www.cdse.edu/documents/cdse/Receive_and_Maint_Sct_Clnc.pdf

Dilanian, Ken. "A Post-Snowden Spying Climate; The NSA Contractor's Leaks Mark a Turning Point in U.S. Intelligence, Experts Say." *Los Angeles Times*, December 22, 2013.

Duffy, Brian, Edward T. Pound, and Gary Cohen. "The Million Dollar Spy." *U.S. News and World Report*, March 7, 1994.

Earley, Pete. *Confessions of a Spy: The Real Story of Aldrich Ames*. New York: Berkley Books, 1998.

———. *Family of Spies: Inside the John Walker Spy Ring*. New York: Bantam Books, 1989.

Egan, Roy. "Former O'Hare TSA Agent, Fired over Repeated Anti-Muslim, Racist Facebook Remarks." *Huffington Post*, November 17, 2011. http://www.huffingtonpost.com/2011/11/17/roy-egan-former-ohare-tsa_n_1099331.html

Ellsberg, Daniel. *Papers on the War*. New York: Simon and Schuster, 1972.

———. *Secrets: A Memoir of Vietnam and the Pentagon Papers*. New York: Viking Press, 2002.

Elsea, Jennifer K. *The Protection of Classified Information: The Legal Framework*. Washington, DC: Congressional Research Service, 2013.

Euske, Kenneth J. and Deborah P. Ward. "The Use of Financial Information in Security Clearance Procedures." Master's thesis, Naval Postgraduate School, 1988.

Federal Bureau of Investigation. "Famous Cases and Criminals—Aldrich Hazen Ames." accessed May 6, 2014. http://www.fbi.gov/about-us/history/famous-cases/aldrich-hazen-ames

———. *The Insider Threat: An Introduction to Detecting and Deterring an Insider Spy* [brochure]. Accessed February 11, 2015. http://www.ncix.gov/issues/ithreat/docs/Insider_Threat_Brochure.pdf

———. "Spies on the Inside: Foreign Intrigue on American Soil." February 14, 2008. http://www.fbi.gov/news/stories/2008/february/espionagecases_021408

Federal Bureau of Investigation Washington Field Office. “Former U.S. Consulate Guard Sentenced to Nine Years in Prison for Attempting to Communicate National Defense Information to China.” March 5, 2013. http://www.fbi.gov/washingtondc/press-releases/2013/former-u.s.-consulate-guard-sentenced-to-nine-years-in-prison-for-attempting-to-communicate-national-defense-information-to-china

Festa, James. P. “New Technologies and Emerging Threats: Personnel Security Adjudicative Guidelines in the Age of Social Networking.” Master’s thesis, Naval Postgraduate School, 2012. http://hdl.handle.net/10945/27829

Finn, Peter, and Sari Horwitz. “U.S, Charges Snowden with Espionage, *Washington Post*, June 21, 2013. http://www.washingtonpost.com/world/national-security/us-charges-snowden-with-espionage/2013/06/21/507497d8-dab1-11e2-a016-92547bf094cc_story.html

Fischer, Lynn F. *Espionage: Why Does it Happen?* Washington, DC: U.S. Department of Defense Security Institute, 1994.

Goldman, T. R. “In the Snowden Case, Bruce Fein Finds the Apex of a Long Washington Legal Career.” *Washington Post*, August 12, 2013. http://www.washingtonpost.com/lifestyle/style/in-the-snowden-case-bruce-fein-finds-the-apex-of-a-long-washington-legal-career/2013/08/11/82ad187a-011b-11e3-9a3e-916de805f65d_story.html

Greenwald, Glen. *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State*. New York: Metropolitan Books, 2014.

Grier, Peter. “Edward Snowden Leaks again: Five Takeaways from the ‘Black Budget.’“ *The Christian Science Monitor*, August 29, 2013.

Grimes, Sandra, and Jeanne Vertefeuille. *Circle of Treason: A CIA Account of Traitor Aldrich Ames and the Men He Betrayed*. Annapolis, MD: Naval Institute Press, 2012.

Harding, Luke. *The Snowden Files: The Inside Story of the World’s Most Wanted Man*. New York: Vintage Books, 2014.

Hartmann, Margaret. “Ahead of His Sentencing, Bradley Manning Says, ‘I’m Sorry I Hurt the United States.’” *New York Magazine*, August 15, 2013. http://nymag.com/daily/intelligencer/2013/08/bradley-manning-im-sorry-i-hurt-the-us.html

Herbig, Katherine L. *Changes in Espionage by Americans: 1947–2007*. Department of Defense Technical Report 08–05. Monterey, CA: Defense Personnel Security Research Center, 2008. http://www.dhra.mil/perserec/reports/tr08-05.pdf

Herbig, Katherine L., Ray A. Zimmerman, and Callie J. Chandler. *The Evolution of the Automated Continuous Evaluation System (ACES) for Personnel Security*. Technical report 13–06. Monterey, CA: Defense Personnel Security Research Center, 2013.

Heuer, Richards J. and Katherine Herbig. *Espionage by the Numbers: A Statistical Overview*. Accessed April 14, 2015. http://www.wright.edu/rsp/Security/Treason/Numbers.htm

Hennessey, Kathleen. "Brazilian President Snubs U.S.; The Key Ally, Angry over Spying Exposed by Edward Snowden, Calls off a State Visit to Washington." *Los Angeles Times,* September 18, 2013.

Hill, Henry J. "Impact of Altering the Delinquent Debt Threshold Used for Background Investigation Expansion on the Denial Rate of Security Clearances." Master's thesis, Naval Postgraduate School, 1991.

Hitz, Frederick P. "The Truth of Espionage is Stranger than Fiction." *Intelligence and National Security* 23, no. 1 (January 2009): 55–60.

Hougan, Jim. *Secret Agenda: Watergate, Deep Throat and the CIA*. New York: Random House, 1984.

Hunter, Robert W., and Lynn Dean Hunter. *Spy Hunter: Inside the FBI Investigation of the Walker Espionage Case*. Annapolis, MD: Naval Institute Press, 1999.

Hurley, Lawrence. "Bryan Underwood, Ex-Security Guard at U.S. Consulate in China, Sentenced to 9 Years for 'Half-Baked Treason.'" *The World Post*, March 5, 2013. http://www.huffingtonpost.com/2013/03/05/bryan-underwood-attempted-treason-sentence_n_2812274.html

Information Security Oversight Office. *2012 Annual Report to the President*. Washington, DC: Information Security Oversight Office, 2013. http://www.archives.gov/isoo/reports/2012-annual-report.pdf

Intelligence and National Security Alliance, Security Policy Reform Council. *Leveraging Emerging Technologies in the Security Clearance Process*. Arlington, VA: Intelligence and National Security Alliance, 2014. http://www.insaonline.org/i/d/a/Resources/LeveragingEmerging_wp.aspx

Johnson, Paul R. "Trusted Insiders are Committing Fraud and Embezzlement within Organizations: Is there a Connection to Addiction, as the Motivating Factor for their Illegal Activities?" Master's thesis, Naval Postgraduate School, 2014.

Jos, Philip H., Mark E. Tompkins, and Steven W. Hays. "In Praise of Difficult People: A Portrait of the Committed Whistleblower." *Public Administration Review* 49, no. 6 (November/December 1989): 552–561.

Knickerbocker, Brad. “Bradley Manning Trial Closing Arguments Ask: Why Did He do It?” *The Christian Science Monitor* (Boston). July 25, 2013. http://www.csmonitor.com/USA/Justice/2013/0725/Bradley-Manning-trial-closing-arguments-ask-Why-did-he-do-it

Kouri, Jim. “Defense Department Official Imprisoned for Espionage.” Renew America. July 16, 2008. http://www.renewamerica.com/columns/kouri/080716

Lefebrve, Stéphane. “The PRC’s Compromise of U.S. Government Information and Technologies.” *International Journal of Intelligence and Counterintelligence* 22, no. 4 (September 3, 2009): 652–666.

Lew, Kimberley. *Introduction to Personnel Security*. U. S. Department of Headquarters, Office of the Chief Security Officer. http://www.iom.edu/~/media/Files/Activity%20Files/PublicHealth/WorkforceResilience/Kimberly%20Lew.pdf

Madrigal, Alexis C. “Bradley Manning, the Person: The Making of the World’s Most Notorious Leaker.” *The Atlantic*, July 13, 2011. http://www.theatlantic.com/technology/archive/2011/07/bradley-manning-the-person-the-making-of-the-worlds-most-notorious-leaker/241920/

Manhattan District History, Security Information Book I-General, Volume 14-Intelligence and Security. September 26, 1952. Federation of American Scientists. http://fas.org/sgp/library/mdhist-vol14.pdf

Maas, Peter. *Killer Spy: The inside Story of the FBI’s Pursuit and Capture of Aldrich Ames, America’s Deadliest Spy*. New York: Warner Books, 1995.

Moynihan, Daniel Patrick. *Secrecy*: *The American Experience*. New Haven, CT: Yale University Press, 1998.

Neuman, Johanna. “Unrepentant Spy Gets 25 Years; ‘I Obeyed my Conscience,’ a Former Intelligence Agency Analyst Says of Her Work for Cuba.” *Los Angeles Times*, October 17, 2002. http://articles.latimes.com/2002/oct/17/nation/na-spy17

Nicks, Denver. “The inside Story of the Oklahoman behind the Biggest Military Intelligence Leak Ever.” *Way Back Machine* [blog]. September 23, 2010. https://web.archive.org/web/20110429142813/http://thislandpress.com/09/23/2010/private-manning-and-the-making-of-wikileaks-2/

Office of the Director of National Intelligence. *Intelligence Community Directive Number 700: Protection of National Intelligence*. Washington, DC: Office of the Director of National Intelligence, 2012.

———. *Intelligence Community Directive Number 701: Security Policy Directive for Unauthorized Disclosures of Classified Information*. Washington, DC: Office of the Director of National Intelligence, 2007. http://fas.org/irp/dni/icd/icd-701.pdf

———. *Intelligence Community Directive Number 704: Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information and Other Controlled Access Program Information*. Washington, DC: Director of National Intelligence, 2008. http://www.dni.gov/files/documents/ICD/ICD_704.pdf

———. *Minimum Standards for Executive Branch Insider Threat Programs*. http://ncix.gov/nittf/docs/National_Insider_Threat_Policy.pdf

Ohlheiser, Abby. "That Time Edward Snowden and Gen. Michael Hayden Took a Photo Together—Wearing Smiles and Tuxedos." *Washington Post*, August 13, 2014.

Olive, Ronald J. *Capturing Jonathan Pollard: How One of the Most Notorious Spies in American History Was Brought to Justice*. Annapolis, MD: Naval Institute Press, 2006.

Popkin, John. "Ana Montes Did Much Harm Spying for Cuba. Chances Are, You Haven't Heard of Her." *Washington Post*, April 21, 2013. http://www.washingtonpost.com/sf/feature/wp/2013/04/18/ana-montes-did-much-harm-spying-for-cuba-chances-are-you-havent-heard-of-her/

Prados, John. "The Navy's Biggest Betrayal." *Naval History Magazine* 24, no. 3 (June 2010): 36–45. http://www.usni.org/magazines/navalhistory/2010-06/navys-biggest-betrayal

Rabechault, Mathieu. "Signs of an Argument before U.S. Base Shooting." *Digital Journal*, April 4, 2014. http://www.digitaljournal.com/news/world/signs-of-argument-before-us-base-shooting/article/379516

Ratnesar, Romesh. "The Unbearable Narcissism of Edward Snowden." *Bloomberg Businessweek*, November 1, 2013. http://www.bloomberg.com/bw/articles/2013-11-01/the-unbearable-narcissism-of-edward-snowden

Reeve, Elspeth. "A Portrait of the Mind of Bradley Manning." *The Wire*, August 14, 2013. http://www.thewire.com/national/2013/08/portrait-mind-bradley-manning/68341/

Relyea, Harold. *Security Classified and Controlled Information: History, Status, and Emerging Management Issues*. Washington, DC: Congressional Research Service, 2008.

Sagar, Rahul. *Secrets and Leaks: The Dilemma of State Secrecy*. Princeton, NJ: Princeton University Press, 2013.

Sarbin, Theodore R., Ralph M. Carney, and Carson Eoyang, eds. *Citizen Espionage: Studies in Trust and Betrayal*. Westport, CT: Praeger, 1994.

Schroeder, Gerald A. “An Overview of Executive Order 12356.” *FOIA Update* 3, no. 3 (1982). http://www.justice.gov/oip/blog/foia-update-guest-article-overview-executive-order-12356

Shannon, Elaine, and Ann Blackman. *The Spy Next Door: The Extraordinary Secret Life of Robert Phillip Hanssen, the Most Damaging FBI Agent in U.S. History*. Boston: Little Brown. Boston, 2002.

Shattuck, John, and Muriel Morrissey Spence. “The Dangers of Information Control.” *Technology Review* 91, no. 4 (1988): 64–73.

Shaw, Eric D., Lynn F. Fischer, and Andrée E. Rose. *Insider Risk Evaluation and Audit.* Technical report 09–02. Monterey, CA: Defense Personnel Security Research Center, 2009.

Shinkman, Paul D. “Defense Paints Bradley Manning as Misguided.” *U.S. News and World Report*, July 9, 2013. http://www.usnews.com/news/articles/2013/07/09/defense-paints-bradley-manning-as-misguided

Sibley, Robert. “The New Spy Game: For Robert Hanssen, It Appeared to be More about a Desire for Recognition than Greed.” *The Halifax Daily News*, February 27, 2001.

Silowash George, Dawn Cappelli, Andrew Moore, Randall Trzeciak, Timothy J. Shimeall, and Lori Flynn. *Common Sense Guide to Mitigating Insider Threats*. 4th ed. Carnegie Mellon University, Software Engineering Institute, 2012.

Sims, Jennifer E., and Burton Gerber, eds. *Transforming U.S. Intelligence*. Washington, DC: Georgetown University Press, 2005.

Sulick, Michael J. *American Spies: Espionage against the United States from the Cold War to the Present*. Washington, DC: Georgetown University Press, 2013.

———. *Spying in America. Espionage from the Revolutionary War to the Dawn of the Cold War*. Washington, DC: Georgetown University Press, 2012.

Swire, Peter. “The Culture War over Snowden.” *Washington Post*. January 30, 2014.

Tajfel, Henri. *Social Identity and Intergroup Relations.* Cambridge: Cambridge University Press, 1982.

Undersecretary of Defense for Intelligence. *Internal Review of the Washington Navy Yard Shooting: A Report to the Secretary of Defense*. Washington, DC: Department of Defense, 2013.

U.S. Department of Defense. *The DOD Insider Threat Program*. Department of Defense Directive Number 5205.16. Washington, DC: U.S. Department of Defense, 2014.

———. *Security from within: Independent Review of the Washington Navy Yard Shooting*. Washington, DC: U.S. Department of Defense, 2013.

U.S. Department of Justice. *A Review of the FBI's Performance in Deterring, Detecting, and Investigating the Espionage Activities of Robert Philip Hanssen*. August 2003. Accessed May 17, 2013. http://www.justice.gov/oig/special/0308/final.pdf

U.S. Department of Homeland Security. *The Department of Homeland Security Personnel Suitability and Security Program*: *DHS Instruction Handbook 121–01-007*. Washington, DC: U.S. Department of Homeland Security, 2009.

U.S. Department of State. *Adjudicative Guidelines for Determining Eligibility for Access to Classified Information*. 2006. http://www.state.gov/m/ds/clearances/60321.htm

Waller, Michael J. "Alive and Kicking." *Insight on the News*, February 18, 2002.

Walsh, Bill. "Arms Analyst Admits Role in Spy Ring: He'll Aid in Prove of 2 N.O. Residents." *Times-Picayune*, April 1, 2008.

———. "Three Arrested in Chinese Spy Plot: Pentagon Official Accused of Passing Weapons Secrets to Local Businessman and Recent Immigrant Cash, Poker Chips Bought Arms Sale Details, FBI Says." *Times-Picayune*, February 12, 2008.

White House. *Protecting Whistleblowers with Access to Classified Information*. (Presidential Policy Directive-19). Washington, DC: White House, 2012. https://www.whitehouse.gov/sites/default/files/image/ppd-19.pdf

———. *Suitability and Security Processes Review: Report to the President*. 2014. https://www.whitehouse.gov/sites/default/files/omb/reports/suitability-and-security-process-review-report.pdf

Whitelaw, Kevin. "Surfing for Secrets: A(nother) Spy Caper." *U.S. News and World Report* 131, no. 8 (September 2001).

Willing, Richard, and Traci Watson. "FBI Portrays Robert Hanssen's Double Life: A 15-Year Paradox." *USA Today*, February 21, 2001.

Wise, David. *Nightmover: How Aldrich Ames Sold the CIA to the KGB for $4.6 Million*. New York: Harper Collins Publishers, 1995.

———. *Spy: The Inside Story of How the FBI's Robert Hanssen Betrayed America*. New York: Random House Trade Paperbacks, 2003.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California