
# NAVAL POSTGRADUATE SCHOOL

**MONTEREY, CALIFORNIA**

# THESIS

**DO INNOVATIVE THINKERS POSE AN INCREASED INSIDER THREAT?: A PRELIMINARY ANALYSIS**

by

Adam Humphrey

June 2019

Thesis Advisor: Gerald R. Scott
Second Reader: Wade L. Huntley

THIS PAGE INTENTIONALLY LEFT BLANK

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



| **1. AGENCY USE ONLY** *(Leave blank)* | **2. REPORT DATE** June 2019 | **3. REPORT TYPE AND DATES COVERED** Master's thesis |
|---|---|---|

**4. TITLE AND SUBTITLE**
DO INNOVATIVE THINKERS POSE AN INCREASED INSIDER THREAT?: A PRELIMINARY ANALYSIS

**5. FUNDING NUMBERS**

**6. AUTHOR(S)** Adam Humphrey

**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.

**12a. DISTRIBUTION / AVAILABILITY STATEMENT**
Approved for public release. Distribution is unlimited.

**12b. DISTRIBUTION CODE**
A

**13. ABSTRACT (maximum 200 words)**

The malicious insider threat is one of the most nefarious of potential cyber security breaches. There have been egregious insider data thefts in the last 10 years within the government. The Unintentional Insider Threat (UIT)—the individual who is incompetent or careless and accidentally divulges sensitive information—is also a major concern. Today, the Department of Defense (DoD) expends considerable effort to identify both forms of insider threats. Meanwhile, the DoD hopes to recruit innovative information technology personnel to better meet current and emerging cyber threats to national security. Although in its infancy, organizations like the Defense Innovation Unit represent this focused effort. This thesis investigates whether innovative personnel will pose increased insider threat potential. Our preliminary conclusion is that innovative people would not pose more of a malicious insider threat, but the UIT and innovator share one trait together: risk taking. Furthermore, mental health issues and disgruntlement are two traits shared by UIT and malicious insiders. The DoD should explore screening personnel for risk-taking traits, for example with the Balloon Analogue Risk Task (BART). Finally, the DoD should continue to be alert to mental health issues, and first line supervisors should intervene quickly to help disgruntled employees.

**14. SUBJECT TERMS**
insider threat, innovation, innovator, cyber security, cyber, data breach, spy, witting insider, unwitting insider, information technology, security, malicious insiders, non-malicious insiders, governance, risk management, compliance, intentional acts, unintentional acts, unintentional insider threat, UIT, personality, trait affect, psychological factors, human factors, cyber security, organizational security

**15. NUMBER OF PAGES**
71

**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.**

# DO INNOVATIVE THINKERS POSE AN INCREASED INSIDER THREAT?: A PRELIMINARY ANALYSIS

Adam Humphrey
Lieutenant Commander, United States Navy
BA, University of Arizona, 2004

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF SCIENCE IN CYBER SYSTEMS AND OPERATIONS**

from the

**NAVAL POSTGRADUATE SCHOOL**
**June 2019**

Approved by: Gerald R. Scott
Advisor

Wade L. Huntley
Second Reader

Dan C. Boger
Chair, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

# ABSTRACT

The malicious insider threat is one of the most nefarious of potential cyber security breaches. There have been egregious insider data thefts in the last 10 years within the government. The Unintentional Insider Threat (UIT)—the individual who is incompetent or careless and accidentally divulges sensitive information—is also a major concern. Today, the Department of Defense (DoD) expends considerable effort to identify both forms of insider threats. Meanwhile, the DoD hopes to recruit innovative information technology personnel to better meet current and emerging cyber threats to national security. Although in its infancy, organizations like the Defense Innovation Unit represent this focused effort. This thesis investigates whether innovative personnel will pose increased insider threat potential. Our preliminary conclusion is that innovative people would not pose more of a malicious insider threat, but the UIT and innovator share one trait together: risk taking. Furthermore, mental health issues and disgruntlement are two traits shared by UIT and malicious insiders. The DoD should explore screening personnel for risk-taking traits, for example with the Balloon Analogue Risk Task (BART). Finally, the DoD should continue to be alert to mental health issues, and first line supervisors should intervene quickly to help disgruntled employees.

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

| | |
|---|---|
| ARPA | Advanced Research Projects Agency |
| BART | Balloon Analogue Risk T |
| CEO | Chief Executive Officer |
| CERT | Carnegie Mellon's Computer Emergency Response Team |
| CIA | Central Intelligence Agency |
| DBIR | Data Breach Investigations Report |
| DIU | Defense Innovation Unit |
| DoD | Department of Defense |
| DoDIN | Department of Defense Information Network |
| MICE | Money, Ideology, Compromise or Ego |
| OPM | Office of Personnel Management |
| SCO | Strategic Capabilities Office |
| UIT | Unintentional Insider Threat |

THIS PAGE INTENTIONALLY LEFT BLANK

# ACKNOWLEDGMENTS

I offer a special thanks to my wife and family for putting up with all the lost weekends and evenings while at NPS. Many thanks to Dr. Wade Huntley for his valuable insight. Thanks to Gerald “Scotty” Scott for taking me onboard.

THIS PAGE INTENTIONALLY LEFT BLANK

# I. INTRODUCTION

## A. RESEARCH QUESTION

Personnel with authorized access are potentially the biggest threat to the Department of Defense (DoD). The cyber actor operating from outside the DoDIN is not as dangerous. The attacker without insider access has to circumvent world-class technology, firewalls, access control lists, intrusion detection systems, and encryption just to *potentially* access sensitive data. In fact, in 2018, insider threats accounted for 28% of all cyber-attacks [1]. Trusted personnel already have the access; they have permission to be "inside the wire." The trusted insider is where the most dangerous threat lies [2].

Meanwhile, the rapid pace of cyber innovation within the DoD is necessitating recruitment of a new type of personnel. As cyber technology continues to evolve, the cyber workforce will need to evolve with it; the DoD will need innovative people to work in it and lead it. The commonplace association of innovative high tech workers with quirky personality types naturally raises the question of whether hiring an innovative workforce will foster more insider threats. The research question this thesis examines in depth is: Do innovative thinkers pose an increased insider threat? A rigorous assessment of this question, going beyond superficial impressions and stereotypes, is necessary to guide DoD policy as it builds a personnel base to meet future information security challenges.

Eric Schmidt, former Google CEO and member of the Defense Innovation Board (as of March 2019), offered testimony to Congress in April 2018 that provides unique insight into DoD innovation. His view is innovators are alive and well within DoD, but the DoD is not postured to adopt new innovations [3]. Innovation happens "in spite of DoD, not because of DoD" [3]. His view that every time there has been bad judgment or performance that DoD has created a rule to prevent it from happening again, but it has created an immovable bureaucracy [3] that is antithetical to innovation. Schmidt also says that talented people leave the DoD or do not work with the DoD because good ideas and innovations are stymied at their inception [3]. He testifies that Defense Innovation Unit

(DIU) successes are more because of "organizational design, culture and degree of autonomy afforded project leaders," than the waivers for some of the more onerous bureaucratic hiring and acquisition hurdles [3]. Schmidt also brings to light his concerns about the need for the department to change its approach to "risk, accelerated timelines and openness to venture innovations" [3]. He concludes with the DoD's need to navigate serious obstacles within its culture, talent management, and processes to be successful at innovation [3]. Schmidt's testimony reveals the need to hire innovators and change the organizational culture of the DoD regarding innovation. To do this successfully, the DoD will need to be confident it is not increasing insider threat potential in the process.

The terms "insider threat" and "innovator" have to be defined as a basis for this research. The DoD definition will be the definition used in this thesis:

> The term "insider threat" means the threat an insider will use her or his authorized access, wittingly or unwittingly, to do harm to the security of the United States. This can include damage to the United States through espionage, terrorism, unauthorized disclosure of national security information, or through the loss or degradation of departmental resources or capabilities. [4]

Utilizing the above definition of insider threat, this thesis will examine both the witting and unwitting insider threats and if they correlate to innovators. Both of the terms "unwitting" and "non-malicious" insider threat will be used interchangeably since most all of the prior research uses non-malicious insider threat or Unintentional Insider Threat (UIT) instead of unwitting [5]. Using the same logic, the terms "malicious" and "witting" insider threat are used interchangeably. It is important to highlight the different terminology, since the use of different terminology among different organizations is prevalent throughout the field of cyber systems and cyber operations.

Most departments within the U.S. government define insider threat in much the same way; the only oddity is the Department of Treasury. The following are the current insider threat definitions of various other departments.

Department of Homeland Security definition:

> An insider threat is defined as the threat that an employee or a contractor will use his or her authorized access, wittingly or unwittingly, to do harm to the security of the United States. [6]
>
> Department of Energy definition:
>
> An insider will use his/her authorized access, wittingly or unwittingly, to do harm to the security of United States. This threat can include damage to the United States through espionage, terrorism, unauthorized disclosure of classified information, or through the loss or degradation of U.S. Government resources or capabilities. [7]
>
> Department of Treasury definition:
>
> It is the policy of the Department of the Treasury to deter, detect, and mitigate insider threats that would do harm to the security of the United States. These efforts include safeguarding classified national security information, while protecting the privacy, civil rights, and civil liberties of Treasury personnel. [8]
>
> National Insider Threat Task Force (NITTF) definition:
>
> Someone who misuses or betrays, wittingly or unwittingly, his or her authorized access to any U.S. Government resource. [9]

As one can see, the definition of an insider threat can be defined in various ways. Definitions can carry multiple meanings and this is particularly prevalent in the cyber, information technology, and computing disciplines. In spite of the differences in how insider threats are defined, all definitions have the essential nature of insider threat in common; a trusted individual has authorized access to information that they use to cause harm to their organization.

In addition to the definition of insider threat, we must define what exactly an innovator is. Defining an innovator or innovative thinker provides a reference point for this research. This thesis will define innovator as, "A creative person [10] who introduces new methods, ideas, or products" [11].

## B. PRIOR WORK ON INNOVATORS AS AN INSIDER THREAT RISK

This thesis focuses on a nexus of research areas that have not been examined together in any depth. There is a plethora of work on insider threats. Additionally, much

work has been completed on innovation. There has not been prior research on innovators themselves having more of a propensity to be an insider threat that has made a significant enough contribution to build on in this thesis.

One work by Olander et al. comes the closest to making a connection between innovators and insider threat, but it does not quite connect the two elements. This work looks closely at "knowledge leaking" and "knowledge leaving" from innovative organizations [12]. It describes how knowledge leaking or leaving intentionally or unintentionally can cause harm to the innovative nature of an organization. However, this work does not make connections to innovators on an individual level having any type of proclivity to becoming an insider threat.

Negative personality traits of the malicious insider threat can also manifest themselves in other ways, such as spying or espionage. While it may not always be the case, research implies there have been cases where these types of acts have aligned closely enough with insider threats to appear as if they fall under the same act: a person with trusted access divulging sensitive, "information to entities who are not authorized to have the information" [13]. Even if espionage involves foreign governments or rival companies, it often requires a trusted insider threat working on their behalf. Almost all of the espionage cases over the last 75 years involved a trusted insider [14]. Of note, some of the insiders did not have clearances, but still had access to sensitive information or had access to people with sensitive information [14].

Background information is needed to understand how the U.S. Government has studied insider threats. In their work for Defense Personnel Security Research (PERSEREC) Center titled, "Americans Who Spied Against Their Country Since World War II," Wood and Wiskoff evaluate every known American spy (read insider) and their motives from 1945 to 1990 [13]. They also build a detailed database that describes specific indicators for the behavior of spies. Congress commissioned the Wood and Wiskoff piece due to the increase in espionage activity during the 1980s [12]. Espionage doubled from the 1950s to 1970 and then doubled again in the 1980s [12]. Their research found that the increase in espionage cases might be a second-order effect of improved counter-espionage tactics [12]. Furthermore, the increase in espionage cases may have

also been attributed to the Carter administration's crackdown on espionage. The crackdown on espionage, may explain the increase in prosecutions related to espionage cases, which also lead to the overall increase in espionage numbers [12], and the current focus in all departments of government on constructing mandatory insider threat programs.

Another component of Wood and Wiskoff's research found that the primary motive for espionage participation was money or financial gain. They conclude that espionage cases were financially motivated 52% of the time [13]. There were 78 spies motivated by money: 16 spied to pay debts, 57 spied for what they termed "simple greed," and the remaining five spied for a combination of greed and debt [13]; nine long-term spies changed their motives to money over time [13]. The Wood and Wiskoff analysis also found the spies with access to classified information often had some gambling, debt or substance abuse problem that drove them to try and steal secrets [13]. Additionally, there have also been 21 cases of ideologically motivated spies; the majority of those were in the 1940s [13]. Another motivation dissected in the Wood piece is that of the disgruntled employee. Since the 1940s 15% of spies have been disgruntled employees.

Financial motivation was not just a relic of the twentieth century, which is why this is an important component to consider when discussing insider threats. Money continues to be the number one motivator of the modern insider threat. The 2018 Verizon Data Breach Investigations Report (DBIR) stated that 76% of data theft was financially motivated [1]. Financial gain is often the determining factor of the driving force behind a person who is an insider threat post WWII [13].

Lynne Fischer's report on insider threat is significant and holds much value for two reasons. First, she discusses Project Slammer, which was a classified program at the time of Fischer's writing, circa 2000. Project Slammer was an effort to interview convicted spies to determine why they committed their crimes. The Project Slammer report has been declassified and provides a discussion on threat characteristics. A key theme in the Project Slammer report is unsaid but can be derived. The convicted spies had little remorse and thought of themselves as entitled, displaying the traits of

psychopathy and narcissism. A key piece of information is that the spies interviewed considered the polygraph to be a key deterrent [15]. Many of the recommendations of the Project Slammer report seem to have been taken onboard by the DoD and her work provides a direct link to insider threat studies conducted by the DoD and the training that was conducted based on those studies [16]. The evidence that DoD derived its training from these reports is the series of video trainings that were produced in the 2000s based on the Project Slammer reports and the PERSEREC reports [16]. Fischer does not state whether the Wood and Wiskoff pieces were utilized in the creation of the training.

Due to the rapid pace of cyber innovation with the DoD, it is essential to examine the relationship between innovation and insider threats. As cyber technology continues to evolve, the cyber workforce will evolve with it and will need innovative people to lead it. This thesis examines if hiring an innovative workforce will foster more insider threats. An analysis of known insider threats and personality traits, and how they correlate to innovative personality traits will help determine if innovators are potential threats. This thesis will help policy-makers evaluate whether innovators pose a genuine insider threat, and if so how to mitigate that challenge while screening and hiring/recruiting the innovative personnel needed to lead, create and implement new cyber capabilities.

## C. METHODOLOGY

Chapters II and III delve into the separate bodies of prior research on insider threats and innovators to distill individual traits associated with both categories that can be compared for correlation. Chapter IV then assesses these groups of traits to identify such correlations. Because there has not been any significant prior research on innovators posing an increased risk of an insider threat, this thesis is creating an original methodology for investigating if such a relationship exists. The analysis in these chapters proceeds as follows:

1. Determine the specific traits for insider threats underlying the DoD definition

The thesis will identify the traits utilized for building training and undertaking counterintelligence investigations. It will then separate sets of traits for witting and unwitting types of insider threats.

2. Determine a specific set of traits associated with innovative personality types

The thesis will carefully look at prior research on innovation at the individual psychological level. A unique set of criteria will be developed for this thesis on the basis of combining contributions from prior research.

3. Correlate insider threat traits to the set of traits generated to depict innovation personality type

Determine the degree to which there are common traits. Examine those common traits more closely to clarify how precisely they overlap. Compare the importance of each trait as an indicator of either insider threat potential or innovative potential (i.e., certain traits may matter more to one than the other).

4. Generate a conclusion as to the overall degree of overlap between insider threat traits and innovative personality traits

If the overlap is relatively small, provide an analysis as to whether innovative personality recruitment can filter traits of concern, and how effectively insider threat training and oversight can mitigate the inclusion of those traits. If the overlap is relatively large, provide an analysis establishing the importance of future research to overcome this dilemma while satisfying DoD requirements for recruitment of innovative personnel.

THIS PAGE INTENTIONALLY LEFT BLANK

# II. INSIDER THREATS

## A. INTRODUCTION

Malicious insider threats tend to make the news, but the non-malicious insider can seriously damage an organization through general human error: accidental disclosure of confidential information, unintentional insertion of malicious computer code, improper handling of sensitive information and lost portable equipment [5]. This chapter will consolidate the applicable scholarship to identify the predominant personality traits and behaviors associated with both the malicious, non-malicious and unintentional (UIT) types of insider threats.

## B. MALICIOUS INSIDER THREATS

The malicious insider is one of the most insidious potential cyber security threats. There have been incredibly damaging insider data thefts in the last 10 years within the U.S. government; most notably the Manning and Snowden data thefts. This section examines the existing literature on malicious insider threat and provides a synthesis of those traits presented in the literature.

### 1. Existing Research

The DoD Insider Threat Integrated Process Team found insider threats to be the majority of personnel who used their authorized access for malicious deeds [17]. They begin with their definition of insider threat:

> Insider threat refers to the ability of an individual or organizational entity to exceed or abuse their authorized access to exploit, attack or otherwise misuse DoD information systems. The insider is different from an outsider because he or she is granted certain authorities and trust. Insiders have superior knowledge of asset value. [17]

The DoD report also states, at the time of its writing, that of 133 intruders into DoD networks, 87% were “employees or others internal to the organizations” [17]. The DoD identified examples of intruders:

> An employee who maliciously altered official medical records on the information system for an individual causing the hospital to cancel a scheduled appointment of surgery for that individual because the medical records could not be found
>
> An employee, by altering information system data, fraudulently routed shipments to a trucking company owned by a friend resulting in the government paying more than $500,000 for hauling freight illegally
>
> A personnel clerk fraudulently entered data into the personnel database attempting to award herself a $500 performance award
>
> A DoD employee obtained an encrypted password file from a DoD classified network and decoded the password file at home. [17]

Although not all of these examples could be construed to be espionage, all were costly. Technical solutions have proven insufficient to detecting insider threats [18]. Computer programs, network anomaly detectors and novel technical solutions are continually being developed within the private sector and government to try and "catch" the insider threat. A greater understanding of the personality traits that drive insider threat behavior would be helpful in improving both technical and non-technical insider threat detection solutions.

An emerging area of study within insider threat psychology are three personality traits associated with malicious insiders that must be examined, they are called the Dark Triad Personality Traits [18]. The Dark Triad traits are Machiavellianism, narcissism and psychopathy [19]. Machiavellianism is a term well known for its negative connotations for unscrupulous behavior. In terms of personality, Machiavellianism is a personality type that manipulates others with, "deception, extreme self-interest and little if any remorse" [18]. Narcissism is a personality trait in which a person is infatuated with himself. The narcissist personality is one that views oneself with inflated self-worth and thinks themselves entitled and superior to others [18]. Psychopathy is trait that presents itself through severely antisocial behavior accompanied by little or no remorse. The psychopathic personality is arrogant, deceitful, impulsive, has low empathy and behaves irresponsibly [19]. These three personality traits presented in one individual would be highly indicative of a potential insider threat.

These Dark Triad Personality Traits are explored by Maasberg et al. in their research on how the Dark Triad relate to the malicious insider threat [18]. Although there is not a large body of empirical research in this area of study, this work does build on prior research [18]. Maasberg et al. utilizes the following insider threat definition: "The insider threat occurs when trusted members of an organization put data, systems, organizations, and even businesses' viability at risk" [18].

Maasberg et al. posits that although technical solutions aid in curbing malicious behavior; they do not get to the root cause of the problem – motivation [18]. Instead, Massberg et al. offers an alternative explanation to insider threats with the Dark Triad theory, together with malicious intent and negative attitude as predictors of insider threat, "viewed through the lenses of the Theory of Planned Behavior and the Capability, Motive, and Opportunity (CMO) model" [18]. For example, after a negative event (e.g., a bad evaluation, demotion, perceived injustice, the hiring of a new supervisor, failure of promotion) a cognitive process is initiated and capable of triggering an insider threat. Maasberg et al. recommends utilizing a Dark Triad personality test much like the Myers-Briggs Type Indicator (MBTI) test and the Adjective Check List (ACL) to identify negative personality traits [18], Maasberg et al. does not elaborate on any other personality tests. Currently, there is no such personality inventory utilized by the DoD during background investigations. This type of testing may prove problematic in practice if it is abused and utilized as a tool to fire someone who may be difficult to work with, but is not an insider threat risk.

In addition to the Dark Triad Personality Traits, Maasberg et al. also restates criticism of the Big Five Personality Model: The Big Five Personality Model includes extraversion, agreeableness, conscientiousness, neuroticism, and openness to experience; however, it does not account for deviant behavior [18]. The Dark Triad personality traits account for the negative traits not present in the Big Five Personality model.

Dupuis and Khadeer also discuss the Dark Triad Personality Traits and how they relate to insider threats. For their research, they define an insider threat as, "an insider threat occurs when trusted members of the organization behave in a manner that puts it at risk." Dupuis and Khadeer go on to define UIT (Unintentional Insider Threat) as; "trusted

employees that [sic] are not seeking to cause harm to their employer; rather, they misuse systems—either intentionally or unintentionally—that results [sic] in some harm to the organization." Although UIT will be discussed in more detail in Section C, it is important to briefly note here, since Dupuis and Khadeer explain how it relates to malicious insider threats. In their research, they attempt to look inside the key concept to understanding the insider threat, and what "motivates" the person who becomes an insider threat [19]. Differing from Maasberg et al.'s views on the Big Five Personality Traits, Dupuis and Khadeer apply them along with the Dark Triad Personality Traits to help determine motivation. A key finding in their research is that UIT and malicious insider threat personality traits are similar in some respects [19].

In his article for the SANS Institute (a recognized expert in cyber security training and certification), Kipp discusses espionage. Kipp claims that espionage is one of the oldest professions, which is why it is important to consider when discussing insider threats. Moreover, he elaborates on his concerns that studies do not diagnose the two most common aspects of every episode of espionage: a betrayal of trust and access to information [2]. Kipp also has an interesting recommendation: he states that companies should spend more time and resources on insider threats than securing their perimeter [2]. Hence, Kipp is making the argument that the insider threat is more dangerous than threats from outside the organization.

Another type of espionage is corporate espionage. In their research, Vashisth and Avinash examine corporate espionage and insider threats [20]. Their definition for acts to be considered espionage is, "an organization or an individual must acquire information considered confidential and important without the knowledge or permission of the party to whom the information belongs" [20]. It is noteworthy that Washington, DC-based companies are hiring ex MI5, CIA, FBI and KGB officers as private investigators to gather information on rivals and their own employees [20]. According to the authors, there are also important variables to consider when it comes to ethical and unethical behaviors:

> Three definitions are important when considering unethical behaviour: 1. A moral issue is present when a person makes a moral decision even if

> they are unaware that moral issues are at stake; 2. A moral agent is a person who takes a decision that may cause harm or benefit; 3. An unethical decision is one that is either illegal or morally unacceptable to the wider community (an ethical decision is the converse). [20]

They also introduce a concept termed MICE, which states that, "spies engage in espionage activities because of money, ideology, compromise or ego (MICE)" [20]. Here "compromise" referred to by Vashisth and Kumar is synonymous with "blackmail." Vashisth and Kumar also look at other theories on why people spy from inside their organizations:

Bad Apple – Individual characteristics determine behavior

Bad Barrel – organizational factors effect unethical behavior

Social Network – interface of social networks effects behavior. [20]

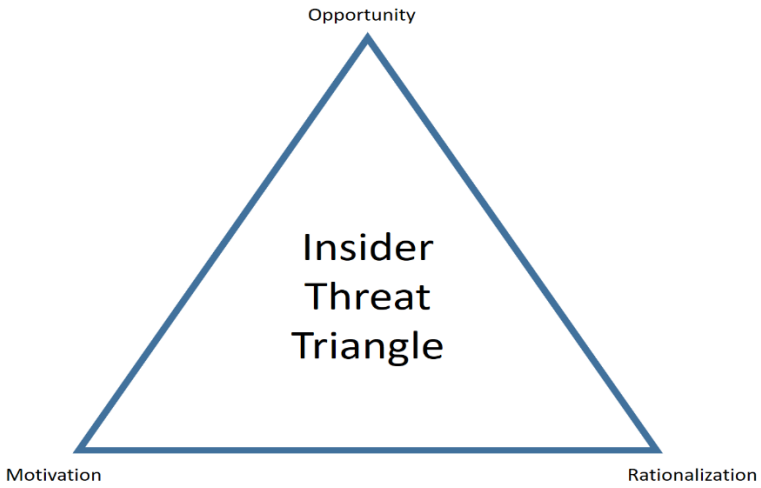
Vashisth and Avinash's research adds to the body of insider threat theories in ways that are different from the other literature reviewed in this thesis. Within the DoD, the Bad Apple theory appears to be most applicable, but will require further research to determine of organizational factors (Bad Barrel) are providing the impetus to personnel becoming insider threats.

A study by Stolfo et al. also addresses the need to study insider threats within an entire organization. Stolfo et al. and his colleagues state that insider threats can be defined as two types, in terms of the cyber domain specifically: "insiders can be divided amongst two non-mutually exclusive classes: Masqueraders (attackers who impersonate another system user) and Traitors (attackers using their own legitimate system credentials) who each have varying levels of knowledge" [21]. Although Masqueraders and Traitors are *not* personality types, it is important to call out the terminology since it does appear in the literature and is yet another example of multiple terminologies for the same cyber phenomena. They argue that technical solutions of access control and policy based-mechanisms have not proven sufficient to eliminate the insider threat problem [21]. The authors also argue in this 2011 piece (two years before Snowden) that the most dangerous insider is probably the user with the most privileges on a system and a high degree of sophistication operating it [21]. The work concludes with the assertion that

more study needs to be done on the security posture of the entire organization, not just user policy [21].

Research conducted by Farahmand and Spafford discuss the "Fraud Triangle," [22] consisting of opportunity, pressure and rationalization. Law enforcement often uses the Fraud Triangle when investigating insider related crime [22]. This thesis proposes to change this slightly to the "insider threat triangle"—opportunity, *motivation*, rationalization.

Figure 1. The Insider Threat Triangle




Adapted from [22]. The insider threat triangle is a way to look what could be the three essential parts of a malicious insider threat

The insider threat triangle could be used to determine the insider threat risks to an organization, much like the "Fraud Triangle" is used by law enforcement as a model to investigate insider crime. Most clearance holders in DoD have access to sensitive information, so the opportunity exists for them become an insider threat. Motivation and rationalization then become two key components at modeling insider threat behavior.

Motivation can also utilize the traits derived from the Fraud Triangle model: "1- Violation of ascribed obligations, 2- Problems resulting from personal failure, 3- Business reversals, 4- Physical isolation, 5- Status gaining, and 6- Employer-employee

relations" [22]. Motivation for an insider threat to act could be reduced by countering the perceived risk by focusing on methods to counter each of the traits above by:

Stressing the importance of obligations to the DoD

Intrusive leadership for employees suffering from a personal failure

Provide financial training to all employees

Promote team-building activities to counter isolation

Emphasize the actual loss of status from becoming an insider threat

Leaders ensuring good morale between leadership and employees. [22]

Furthermore, Farahmand and Spafford explain perceived risk and rationalization among insider threats. Risk rationalization threats view themselves as, "1) essentially noncriminal, 2) justified, and 3) part of general irresponsibility for which they do not feel accountable" [22]. This same rationalization was also present in the Project Slammer report [15]. According to Farahmand and Spafford, when it comes to perceived risk and rationalization, "the higher the perceived benefit, the lower the perceived risk, and vice versa—is strengthened greatly under time pressure" [22]. They also add, "Insiders normally make decisions based on change of wealth rather than total gain (i.e., values, perceived by insiders, are attached to changes rather than to final states, and that their decision weights do not coincide with stated probabilities)—a behavior that is well explained by "Prospect Theory" [22], [23]. Prospect Theory explains the way people perceive risk when the probabilities of outcomes are uncertain. This insight explains the insider threats' financial gain motivation.

The authors mention that deterrence of (malicious) insider threats can be effective if the insider thinks they are going to be discovered before they can execute their crime. This explains why the convicted spies viewed the polygraph as a deterrent [15]. They also argue, "that fairness and justice are factors that affect employees' actions within organizations," [22]. Farahmand and Spafford conclude, "Making effective decisions to confront insider threats requires understanding insiders' risk taking behavior and their decision heuristic" [22]. The ability of the cybersecurity apparatus, in a holistic manner,

to understand the insider threat's decision framework is critical in determining an individual's propensity to be an insider threat.

It should be mentioned that Farahmand and Spafford agree with other researchers by stating that there is not a universally agreed upon definition of insider threat [22]; but, at the same time, this work does not distinguish between UIT and intentional insider threat. Such a distinction would have been helpful to apply this work to determine the trait differences between UIT and the malicious insider. Accordingly, much of this work informs the following section as well.

There are also social components to consider when it comes to insider threats. For example, culture has a lot of influence on perceived risk as well [5]. Carnegie Mellon University's "The CERT (Computer Emergency Response Team) Insider Threat Team" (referred to as CERT throughout the rest of this thesis) has the most comprehensive report on UITs in the literature [5]. CERT states, "Cultural beliefs, social relationships, power relationships, hierarchies, knowledge, experience, discourse, and practice all influence perceived risk" [5]. An example of this perceived risk in an organization is Wall Street investment bankers; there is a correlation between investment banker culture and the increased risks they take to make money for clients [5]. Gender, mood and familiarity with risk are also examined by the CERT report. There have been 150 studies that have shown, "men are more likely to take risks than female participants" [5]. Unfortunately, the research on mood, "has been inconsistent in determining risk-taking behavior" [5]. Third, someone who is in consistent contact with the same risk may become so used to the risk that they no longer identify it as a risk [5].

### 2. Synthesis of Traits Common to Malicious Insider Threats

A set of "negative" personality traits can characterize the insider threat. The Big Five inventory is a good model of easily identified personality traits, e.g., neuroticism, agreeableness, extraversion, conscientious and openness to experience [18]. The traits in question are the Dark Triad traits. These are the personality traits that might be tested for in DoD employees.

The following is the complete set of malicious insider traits derived from the preceding assessment:

- Machiavellianism – Dark Triad
- psychopathy – Dark Triad
- narcissism – Dark triad
- anti-social
- addictive/compulsive/destructive behavior
- mental health issues
- seizure disorders
- risk aversion
- panic attacks
- rebellious
- passive aggressive
- introverted
- paranoia
- ethical flexibility
- gender confusion
- greed/financial gain
- disgruntlement
- passive aggressiveness
- financial need

## C. UIT INSIDER THREATS

As mentioned previously, UIT are personnel who are careless or subvert security policy, but do not wish to intentionally harm the organization. Out of all reported data breaches, UIT insider threats were responsible for 17% of insider threat data breaches [1]. These included instances of misconfigured IT equipment, email sent to the wrong address and not following procedures for the handling of sensitive information [1]. The following sections in this chapter will review existing literature on the UIT and provide a synthesis of the UIT traits.

### 1. Existing Research

The following is an example of an unwitting insider threat that intentionally violates procedures without the intent to harm the organization. This example displays the human error portion of an unwitting insider threat. There was an FBI agent who was a foremost expert in counter terrorism within the U.S. government. Attorney General Janet Reno considered him to be one of the most competent men at his job [24]. This man proved to be an unwitting insider due to multiple instances of non-procedural compliance. On three separate occasions, he violated procedures that proved to be a direct threat to FBI property and information. Initially he lost an FBI cell phone and palm pilot. Then the second violation occurred when he took a vehicle from an FBI safe house without permission when his car broke down. Thirdly, he took classified documents from his office (which is a violation of procedure) and lost them for a few hours when he accidentally left a briefcase in a public conference room. This example of an unwitting insider is not to focus on incompetence, but the opposite. Even the most operationally competent employee can be an unwitting insider threat [24]. An unwitting insider may in fact be a competent employee who does not always follow procedures.

This example shows that, although UIT personnel may make honest errors with no malicious intent, their acts may still be held against them. Even though an FBI agent was considered the foremost expert in counter terrorism, his UIT actions still caused his career to end early [24].

Carnegie Mellon University's CERT report defines UIT as

> An unintentional insider threat is (1) a current or former employee, contractor, or business partner (2) who has or had authorized access to an organization's network, system, or data and who, (3) through action or inaction without malicious intent, (4) causes harm or substantially increases the probability of future serious harm to the confidentiality, integrity, or availability of the organization's information or information systems. [5]
>
> CERT's report looks at the human performance failure into four root causes:
>
> Data flow- inadequate procedures, poor communications
>
> Work Setting – Distractions, insufficient resources, inadequate security practices
>
> Work Planning and Control: Task pressure, difficulty, poor planning, lack of knowledge or skill.
>
> Employee Readiness: Stress, inattention, anxiety, boredom, illness, drug and hormone side effects, attitude, values and other cognitive issues. [5]

According to CERT, UIT had not been specifically studied up until their report [5]. CERT discusses the challenging terminology differences explaining the same insider threat phenomenon, for example, "unintended insider threat, accidental insider threat, and inadvertent insider threat" [5]. CERT also claims that common factors with malicious insider threats do not easily map to UIT. CERT examines the notion of human error through "proximal relationships between the sharp end (those in contact with critical processes) and the blunt end (shapes drives and supports the sharp end)." CERT argues that the blunt end creates constraints and pressures on the sharp end that creates opportunities of what they term as "human performance errors."

CERT researched the lack of situational awareness and "mind wandering" as factors that can lead to UIT [5]. Mind wandering creates a decoupling of conscious thought to current tasks, creating errors [5]. Lack of situational awareness causes a person not to, "perceive relevant information because of distracting tasks," failure of situational awareness was a factor in 71% of air traffic control failures [5]. In terms of UIT, a failure in situational awareness can lead to a computer user clicking on malicious links because they do not perceive the danger [5].

Regarding an individual's ability to evaluate risk, the CERT report also heavily references Kahneman and Tversky's Prospect Theory, which won the Nobel Prize in Economics. The experiments used in Kahneman and Tversky's research were, "a series of gambling experiments to show an irrational behavior in evaluating probabilities and introduced heuristics and biases which may lead to inaccurate judgments" [5]. In other words, a person's biases make them poor at evaluating risks [5]. CERT also provides evidence that risk reevaluation is poorly implemented as new information is received due to confirmation bias [5]. Essentially, confirmation bias is discarding pieces of information that do not confirm participants' Plan "A" (CERT uses ship Captains as an example) [5]. This leads to risk being evaluated against Plan "A," when reality is actually Situation "B" [5].

Based on the literature, CERT discusses a possible way to measure employee risk- taking behavior with an instrument called the Balloon Analogue Risk Task (BART) [5]. BART is computer- and lab-based instrument which measures a employees tolerance for risky behavior [5]. CERT discusses how prior research correlated risky behavior with the Big Five Personality Traits (extraversion, openness, neuroticism, agreeableness, and conscientiousness) specifically, with extraversion and openness. There was a low correlation with neuroticism, agreeableness, and conscientiousness [5]. The BART test may be worth investigating as a tool to screen for risky behavior that could lead to an insider threat. If an excessive risk taking employee could be identified, controls and mitigations could be put in place [25] to reduce the possibility of a UIT incident to DoD.

Research conducted by Farahmand and Spafford also examine the risk-taking behaviors of insider threats [22]. This research is an important component because it determines that risk-taking behavior appears to be one of the only traits UIT may have in common with innovators. Additionally, Farahmand and Spafford's research also observes how Kahneman and Tversky's Prospect Theory explains irrational behavior and inaccurate judgments. Another vital component to Farahmand and Spafford's research examines constructs of risk perception:

> Does the insider voluntarily get involved in the risk situation (voluntariness)?

To what extent is the risk of consequence from the insider's action to him/her immediate (immediacy of effect)?

To what extent are the risks known (precisely) by the insider who is exposed to those risks (knowledge about risk)?

To what extent are the risks precisely known and quantified (knowledge to science)?

To what extent can the insider, by personal skill or diligence, avoid the consequences to him/her while engaging in the untoward activity (control over risk)?

Does the risk affect the insider over time or is it a risk that affects a larger number of people at once (chronic-catastrophic)?

Are these risks new to the insider or is there some prior experience/conditioning (newness)?

Is this a risk that the insider has rationalized and can think about reasonably calmly (common-dread)?

When is the risk from the activity realized in the form of consequences to the insider (severity of consequences)?[1] [22]

This attention to risk propensity identifies an important element of UIT insider threat traits that may relate to innovative personality types.

### 2. Synthesis of Traits Common to Unintentional Insider Threats

There are not as many UIT traits as the malicious insider threat traits. The common UIT traits derived from the literature can be narrowed down to [5], [19], [25]:

- disgruntlement
- mental health issues
- carelessness
- risk taker

[1] Future research could replace the words in the above list with "insider" with "innovator" and the word "untoward" with "creative" to test an innovator's risk perception.

These traits are not surprising given the non-malicious nature of the UIT, and will be discussed with the "organization" being the DoD. A disgruntled employee may not work with the same sound decision making as an employee who is not disgruntled [25]. Mental health issues can also contribute to careless behavior which could inadvertently harm [5], [25] the organization. Although it seems obvious, increased risk taking by an employee could result in a myriad of negative consequences [25]. Carelessness from a UIT can result in negligent actions that can cause damage to the organization [5] .

The only trait above that overlaps with the traits of innovators is risk taker [5], [10], [25]. Although a typical innovator may be thought of as careless (Elon Musk smoking cannabis on Joe Rogan's podcast for example—resulting in a significant drop in Tesla stock [26]), the literature does not identify carelessness as a trait in innovators [10],[27],[28],[29] (see the discussion in the following chapter).

## D. CONCLUSION

This chapter has examined existing research on insider threats to distill this research into two sets of personality types associated respectively with malicious and non-malicious insider threats. These sets of traits will provide the basis, in Chapter IV, to investigate possible correlations between these traits and the traits of innovative personalities developed in the following chapter. Prior to moving to that discussion, this chapter concludes with observations concerning possible DoD applications of the analysis of the current chapter.

The notion of an individual displaying traits from Dark Triad of Machiavellianism, psychopathy and narcissism could shed light on an employee at risk of becoming a malicious insider threat. Conversely, the UIT is often a careless person [5]. A person displaying more than one UIT trait (e.g., an employee who has propensity to take unnecessary risks, and is disgruntled) should cue front line supervisors to step in and help the employee mitigate their issues. Life stressors can trigger latent malicious insider threat traits in potential insider threats [30]. It is incumbent on leaders to identify personnel with significant life stressors that make them distracted and prone to careless mistakes of an UIT. Risk-taking propensity is also key in identifying the UIT. The BART

could be used by DoD to identify at job applicants that may be too prone to risk taking before they are even hired.

The Fraud Triangle is used by law enforcement to investigate insider crime [22]. A slight modification to the Fraud Triangle could make it useful for cyber professionals to derail a potential malicious insider threat. If one leg of the triangle could be removed, then the insider threat may not act.

THIS PAGE INTENTIONALLY LEFT BLANK

# III. PERSONALITY TRAITS OF INNOVATORS

## A. INTRODUCTION

To determine if innovators pose more of an insider threat, it is essential to have a clear understanding of the personality traits associated with an innovative individual. The dictionary definition of an innovator is "a person who introduces new methods, ideas, or products" [11]. However, the personality traits of actual innovators are much more nuanced.

This chapter presents the most important prior work on identifying and describing the personality traits associated with innovation. The chapter then utilizes this work to generate a set of traits that his thesis, in the following chapter, can compare to the insider threat traits developed in the preceding chapter.

## B. INDIVIDUAL LEVEL PERSONALITY TRAITS

The definition of innovator can be problematic, since the term is used ubiquitously throughout our modern society, and the definition has become "watered down" [31]. Kirton defines an innovator as, "the creative person (a) has little awe of traditional knowledge or practice; (b) compulsively toys with ideas; and (c) displays a high need for social recognition, that is, wants his ideas to be judged good, without regard to their latent or manifest heretical challenge to consensus" [10].

### 1. Existing Research

Michael Kirton's seminal 1976 paper called, "Adaptors and Innovators: A Description and Measure" derives multiple behavioral traits from 532 people classified as "innovators" or "adaptors" [10]. Kirton's original work examined the personality traits of innovators; he discovered what we often call today "disruptors." Innovative personnel, as Kirton defined them, do not get along with the status quo [10]. According to Kirton, if the innovator saw a problem, he began to look for novel solutions, even if those solutions disturbed the established order of the organization [10].

Kirton identifies an innovator through a series of behavioral traits. He describes an innovator as a person who:

Finds problems and solves them:

- Is a disruptor to groups who have been established
- Is viewed as impractical and shocking to people who are less innovative
- Questions assumptions and manipulates problems
- Delegates routine tasks quickly and works in bursts
- Does not really regard established means when pursuing a goal
- Has little doubt about his ideas and does not require consensus
- Will take charge in an unstructured environment
- Has little regard to past custom and will challenge the rules
- Thrives in a crisis but is also well versed at avoiding crises; if they (the innovator) can be controlled
- Is often a threat to group cohesion and is insensitive to people
- Has potential to bring about substantial change within a stagnant group or organization. [10]

Sandberg et al. define innovativeness as, "the ability successfully to implement creative ideas in order to make a specific and tangible difference in the domain in question" [29]. They go on to define innovator as "a person who is able to create and/or is willing to try out a new idea before others do so" [29]. According to Sandberg et al., the characteristics of innovators are:

- Risk-taking propensity
- High tolerance of ambiguity
- Persistence
- Self-efficacy

- Willingness to change
- Curiosity and interest in problem solving. [29]

Smith and Richardson defines innovation yet another way: “Innovation is by definition novelty. It is the creation of something qualitatively new via processes of learning and knowledge building. It involves changing competences and capabilities and producing qualitatively new performance outcomes” [32]. Smith and Richardson add questions to their definition, “Does an innovation have to incorporate a radically novel idea, or only an incremental change? In general, what kinds of novelty count as an innovation?” [32]. Smith and Richardson also argue that innovation is a multidimensional rather than linear process, and many aspects of its processes are very hard to measure [32].

Scott and Bruce in their work on the determinants of innovative behavior argues that an innovative individual (innovator) utilizes three steps in the innovation process: 1) seeks sponsorship, 2) builds a coalition and 3) then creates a prototype that can be manipulated [33]. Scott and Bruce go on to posit that innovation is completed in discontinuous steps and looks at catalysts to innovative behavior: an organizational bias to creativity and positive leader and workgroup climate [33].

Scott and Bruce also analyze the thinking behind innovation and innovators. She talks about bisociative thinking which has, “overlapping separate domains of thought simultaneously, a lack of attention to existing rules and disciplinary boundaries, and an emphasis on imagery and intuition. We call this mode the intuitive problem-solving style” [33]. Scott also discusses the “Pygmalion” effect which is an effect where others expectations of a person affect that person’s performance, e.g., a manager thinks a person is incapable of doing a good job, so that person does not perform well. She concludes by stressing the difficulties of studying individual workplace behavior because the criteria are difficult to measure and the researcher is, “limited to the use of perceptual measures” [33].

Agarwal et al. study innovative behavior in their paper through the willingness of people to adopt new information technology. They describe innovative personnel as

"change agents" and "opinion leaders" whose use of new IT promotes "further diffusion" of the technology [27]. This definition is yet another on personal innovation.

Many people who are considered innovators have the traits described above. Alan Turing was described by his biographer Andrew Hodges: "Alan was slow to learn that distinct line that separated initiative for disobedience" [31]. Vinton Cerf, one of the inventors of the internet, is also an innovator who fits Kirton's innovator trait definitions. Cerf would wear a coat and tie to school to standout: "I didn't want to fit in with everyone else" [31]. Another trait Cerf displayed from Kirton's research on innovators is the ability to establish a group to accomplish a task out of nothing. Cerf and Robert Kahn had an idea to create a network that anybody could join, with various computer nodes that could transfer data among the computers of the connected network. Cerf organized a meeting at Stanford to move this idea forward exactly as an innovator would "take control of an unstructured situation" [10], [31]. Interestingly, there is not a mention of Turing or Cerf displaying a propensity to become an insider threat. These men were innovators and mavericks but not disloyal to their organizations.

### 2. Synthesis of Traits Common to Innovators

The preceding works are a sampling of some of the myriad of traits for innovators found in research on the topic. The list below is a summary compilation of those traits [5], [10], [15], [18], [19], [25], [27] [29], [30], [34]:

- Altruistic
- Trust
- Persistent
- Willingness to Change
- Disruptor
- Self-Efficacy
- Insensitive
- Abrasive

- High Tolerance for Ambiguity
- Committed to The Organization
- Creative
- Intuitive
- Risk Taker

Each innovator does not have all of these traits [35]. Some innovators embody almost all of these traits, and some have only a few. Much like insider threats, there does not seem to be a typical innovator. However, throughout this research, innovators do seem to have two traits in common out of all the listed traits listed above: risk-taking and openness to experience [22], [35]. Referencing the Big Five personality traits (neuroticism, agreeableness, extraversion, conscientious and openness to experience), openness to experience seems to have the highest correlation with creativity [35], and creativity is the essence of innovation. Therefore, there are really three fundamental traits associated with innovators, "creativity, openness to experience and risk taking" [35].

## C. TRAITS OF ORGANIZATIONS THAT FOSTER/IMPEDE INNOVATION

### 1. Existing Research

Hölzle et al. write about the personal characteristics of innovators and their roles in innovation management [34]. They argue the innovator needs autonomy, independence from organizational regulations and the latitude for spontaneity and self-determination, which facilitates creativity [34]. They also discuss the different models of innovation management via the champion model and the promoter model [34]. The champion is a single person who gets behind the innovator and their product, pushing it through the organization [34]. The "promoter model" includes four different types of promoters: the expert promoter (specific technical knowledge), the power promoter (has hierarchical power) and the process promoter (can expertly navigate the organizational processes), relationship promoter (links expert and power promoter) [34]. This model, "has a long research tradition in German speaking countries." [34]. A key point in this work is the assertion, with the caveat that the organization studied was specifically research and

development, that innovators are: “employees with a strong organizational commitment [who] exhibit a high acceptance of the goals and values of their organizations and are willing to put in considerable effort on behalf of their organization, as well as possess a strong desire to remain a member of their organization” [34].

The innovators’ commitment to the organization is the polar opposite of the insider threat, who is subverting their organization.

As mentioned in Chapter I, Olander et al. argues that proper management of knowledge leaking and leaving within the company prevents knowledge from being shared outside the company, thus maintaining the prerequisites for innovation within the company itself [12]. This notion of knowledge leaking and leaving both intentionally and unintentionally is important to realize, as knowledge management relates directly to innovation and tangentially to insider threat. Organizational trust is also important when it comes to preserving the prerequisites to innovation. Olander argues that employees’ trust in the organization makes policy enforcement less difficult since employees will more likely adopt policy when they believe management is looking out for their best interests and can be trusted [12]. This research suggests that innovators would support DoD policies to thwart insider threats, an inclination antithetical to being insider threats themselves.

Velasco et al. focuses on the role the organization plays in creating an innovation friendly atmosphere. This work emphasizes particularly the role “human resource policies, strong leadership and a robust innovation culture play in mobilizing full innovative potential” [28]. Although it seems intuitive, their paper speaks to the negative impact that time and resource constraints have on innovative behavior [28].

Organizational processes can also have a profound impact on innovation, especially in the DoD [3]. Suzanne Scott and Reginald Bruce’s work on innovative behavior discovered that organizational support for innovation, leadership, managerial expectations, systematic problem solving and career stage all played a significant role in innovative behavior [33]. The reasons identified in the previous sentence are logical since the most innovative person in the world can be kept locked into stifling

organizational processes by leadership and management that are unwilling to provide support to innovation.

With any new method, idea or product there is going to be change. Most people readily accept organizational change [33]. Innovators are not necessarily concerned with organizational norms or entrenched processes. Thus, the innovator will seek out and solve problems in a way that may make others uncomfortable [31].

### 2. Key Traits of Organizational Innovation

Understanding the key traits of organizations that support an innovative climate are directly relevant to DoD efforts to enhance recruitment of innovative personnel. The research considered in this Section can contribute to those efforts. With respect to the association of innovator personality traits to insider threats, this organization-level research indicates that promoting a culture that supports innovation while also combatting insider threats may be mutually reinforcing objectives for the DoD.

## D. CONCLUSION

The two preceding sections point to important observations. Innovators are agents of change who take a new idea or process and disrupt the status quo within their organization. At the same time, innovators can display high levels of loyalty to dynamic organizations that support an innovative culture. In the following chapter, the thesis will examine if there is a correlation between the synthesis of traits common to innovators and the synthesis of traits common to insider threats.

THIS PAGE INTENTIONALLY LEFT BLANK

# IV. ARE INNOVATORS INSIDER THREATS?

## A. INTRODUCTION

If an organization is innovating, it is developing new ideas and processes with the changing times [10]. An example of innovation in spite of DoD bureaucracy can be witnessed by ARPANET, the original internet. ARPANET was created to link laboratories together so they could share computing resources [36]. This innovation changed drastically from its original form as it evolved into the ubiquitous internet that we all utilize today. The inventors of ARPANET were innovators, but did not display more propensity to be an insider threat [36], [37].

ARPANET is only one example of successful fostering of innovation within the DoD. Recruitment of innovative personnel to meet information security and cyber security challenges can be another successful example. To facilitate that success, the following discussion draws together the findings of the prior two chapters to discern how innovative personnel recruitment will impact insider threat potential.

## B. TOP LEVEL FINDINGS

Figure 2 presents the basic findings of this thesis concerning correlation of personality traits of insider threats developed in Chapter II with personality traits of innovative individuals developed in Chapter III. Malicious insider threat traits are collected on the upper-right side of the figure. Non-malicious insider threat traits are collected on the lower-right side of the figure. Personality traits of innovative individuals are collected on the left side of the figure. Traits that are more divergent or contradictory between innovators and insider threats are represented visually by horizontal separation in the figure. Traits that are more convergent or overlapping between innovators and insider threats are suggested visually by location closer to the horizontal middle of the figure; these traits are enclosed in boxes between which there are connecting lines.

Figure 2. Correlation of Traits

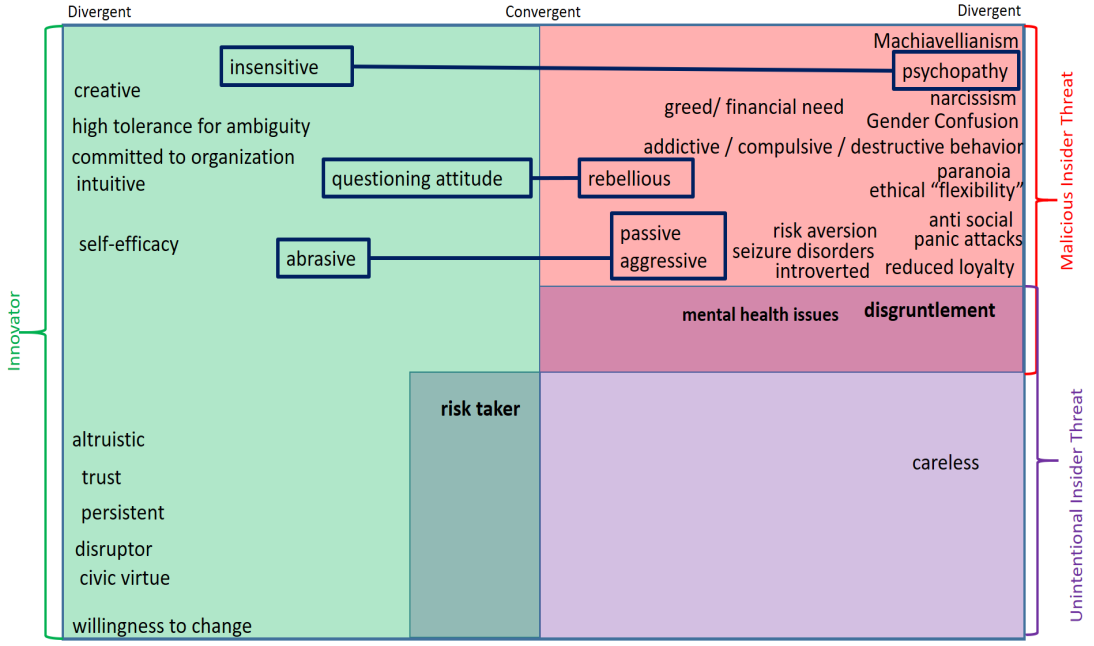



Figure 2 is a depiction of overlap of UIT, Malicious Insider Threat and Innovator traits. Adapted from [5], [10], [15], [18], [19], [25], [29], [30], [34].

As the representation in this figure displays, there is little convergence between the personality traits of insider threats and of innovators. In conjunction with the finding in Chapter III that innovators also often display organizational loyalty, the basic conclusion of this thesis is that innovative individuals, in general, should not be considered insider threats, and in fact would likely support efforts to minimize insider threat potential within the DoD.

This overall conclusion is not absolute. Figure 2 identifies several pairs of traits that may be convergent between innovators and malicious insiders. Figure 2 also displays a possible relationship between risk-taking propensities of innovators and unintentional insider threat.

The following two sections examine in more detail the association of the traits of innovators with, respectively, those of malicious and non-malicious insider threats.

## C. CONVERGENCE AND DIVERGENCE OF MALICIOUS INSIDER THREAT TRAITS AND INNOVATION TRAITS

Overall, it is clear that most of the personality traits associated with innovators and malicious insider threats are divergent. The divergence of innovators and malicious insider threats occurs most fundamentally in their relationship to acceptance of risk. Farahmand and Spafford state that "risk aversion is the reluctance of an insider to accept a bargain with an uncertain payoff rather than another bargain with more certain, but possibly lower expected payoff" [22]. Clearly, there is no cumulative convergence (overlap) in the traits of innovator and the traits of insider threat.

Of course, human beings are unique and individual; there is no archetypical innovator and there is no typical insider. Considering all of the traits identified in Chapters II and III, only three sets show convergence of malicious insider threat traits and innovator traits, displayed in the following table:

Table 1. Potential Trait Convergence

| Innovative Trait | Malicious Insider Trait |
|---|---|
| Insensitive | Psychopathy |
| Questioning attitude | Rebellious |
| Abrasive | Passive aggressive |

As Chapter III noted, innovators may express any subset of traits from within the longer list associated with innovative personalities [35]. Some innovators may express only a few of these traits, and none are typical. This raises the possibility that certain innovators may also be insider threats. But a closer look at each of these pairs shows that such convergence would not be typical.

Innovators may be insensitive [10] but they are *not* insensitive to the point of being psychopathic, e.g., completely disregarding the feelings of others and lacking remorse. Malicious insiders are much different; they only have remorse for themselves and the fact they got caught [15], and they do not care about the negative impact of their actions had on national security [15].

Innovators question the status quo often [10] but are not in full rebellion against it. They are working create something new or different and without damaging the organization for which they are working. Malicious insiders are in a full state of rebellion. Although greed, not hurting the organization, is the insider's usual motive, the insider is using their trusted access in a way that will hurt their organization. They are not merely displaying a questioning attitude; the malicious insider is knowingly engaging in activities that will undermine the organization.

An innovator is often abrasive, as their new creation is changing, or could change something people are comfortable with. The passive aggressive person is not necessarily overtly abrasive. This possible association between passive aggression of the malicious insider threat, and abrasiveness of an innovator, requires more research.

In contrast to these three semi-convergent sets of traits, diverging traits of innovators and malicious insider threats are many and wide ranging. The destructive traits of a malicious insider (Dark Triad, ethical flexibility, reduced loyalty) are on the other end of the spectrum compared to the constructive traits of the innovator (altruistic, civic minded, trust, committed to the organization).

Innovators are agents of change [10], the essence of an innovator is creating change. They seem to always do this within the confines of their organization – whether the organization is a multinational corporation or one person in their garage. Thus, there does not appear to be much if any threat from an innovator "burning down" the organization like Snowden and Manning did with their data breaches promulgated with insider access. When one analyzes the definitions of narcissist, psychopath and Machiavellian personality traits [18] Snowden and Manning's actions strongly resemble these Dark Triad personality traits.

It is worth examining the Edward Snowden case, since it is a case of a technically sophisticated insider threat causing great harm to the DoD by divulging a large amount of classified data. Edward Snowden was an NSA contractor who covertly exfiltrated 1.5 million classified documents from NSA databases without permission and posted them online in June 2013 [38]. After he stole the documents he absconded to Hong Kong to meet with

*Guardian News* reporters [38]. His goal was to gain asylum in Germany, which was denied [38]. Snowden was eventually granted asylum in Russia by Vladimir Putin [38].

Although he was not psychoanalyzed in person [30], Snowden displayed all the Dark Triad personality traits. He thought of himself as a great person (narcissism) [38], he didn't care who was hurt (psychopathy) [38] and he snuck the data out of NSA field offices and met reporters in Hong Kong (Machiavellianism) [38]. The Dark Triad traits are very dissimilar to the traits of innovators, with the exception of one, insensitivity. Insensitivity is slightly related to psychopathy, since psychopaths by definition are insensitive to other people; psychopaths are not empathetic to others [18]. Snowden displayed two innovator traits: "questioning" and "abrasive." Nowhere in the literature is he described as "creative." He definitely was not "committed to the organization," "trustworthy" or "altruistic," all traits displayed by innovators.

A distinct example of someone who was both an innovator and insider threat is Klaus Fuchs (pronounced Fukes). Fuchs was literally at ground zero during the development of the atomic bomb, as he was present during the Trinity Test. He was a theoretical physicist who left Germany when the Nazis took power. His case is different than those other innovators because his family were extreme ideologues and were intimately involved in German socialist politics [31].

Fuchs was as deep an insider threat as one can be. His participation in atomic development included bleeding edge calculations on implosion triggers of fissile material and alloy tube construction for atomic weapons; among other contributions [31]. He was allowed access to the most sensitive meetings and collaborations during the creation of the atomic bomb [31]. He was one of the leading innovators behind the atomic bomb and also one of the biggest insider threats in history. Fuchs used his trusted access to sensitive information and passed detailed reports and plans on the Manhattan project to Soviet intelligence officers [31].

The trait that makes Fuchs an outlier was reduced loyalty because he was an extreme ideologue and believed whole-heartedly in the Soviet System. Many of the U.S. persons who were spies during WWII and shortly after were spying based on ideology [13].

The Fuchs case shows that an innovator can be a malicious insider threat; the convergence is not impossible. But the analysis of this thesis also shows why that convergence should be the exception, not the rule. Moreover, by identifying the few specific traits of innovators that might converge with malicious insider threats, this thesis provides guidance for the DoD to identify those traits in its recruitment practices. Because these traits are far from essential to successful innovators, screening for them should not impede innovation recruitment.

## D. CONVERGENCE AND DIVERGENCE OF UIT AND INNOVATOR TRAITS.

The literature does not support a convergence of most UIT traits with innovators, with one exception: *risk taking* [5],[29]. The malicious insider is risk averse, evincing "the reluctance of an insider to accept a bargain with an uncertain payoff rather than another bargain with more certain, but possibly lower expected payoff" [22]. The UIT is just the opposite. The UIT risk-taking trait is prevalent because an employee may risk possible malware infection for speed and efficiency of completing a task (CERT).

Creativity and the ability to implement creative ideas is the root of an innovator along with risk [29]. Inventors create new technology; the innovator is the person who can create *and* implement the technology. Elon Musk worked to create viable electric vehicle technology; the difference is that he implemented the technology. Implementation is what separates inventors from innovators. Risk-taking is also a characteristic of the innovator. Moreover, innovators are not concerned with disturbing the status quo to further their innovations. They will create and implement regardless of how others feel about their methods.

Thus, DoD should be concerned with screening for creativity and the ability a person has displayed to implement their creativity. The UIT risk determination can be measured by using the Balloon Analogue Risk Task (BART) computer-based test that can predict risk-taking behavior [5]. BART has been effective in identifying risk-taking behavior (CERT) and could be a way for DoD to help identify individuals prone to risk-

taking behavior. These individuals could then be counseled and supervised differently to ensure they exhibit less UIT type behavior.

## E. CONVERGENCE AND DIVERGENCE OF INNOVATIVE ORGANIZATIONS AND MILITARY ORGANIZATIONS

Considering the rapid pace of cyber innovation and the rapidly changing nature of cyber systems, the DoD must hire highly innovative personnel to keep up, thus adding to the complexity of the insider threat problem in two ways. First, the DoD must be able to attract innovators, and, second, the DoD should explore ways to identify innovators who might also be insider threats. Both are discussed in this section.

Currently, the DoD hiring process is not conducive to hiring innovative personnel. In fact, in a search for the word innovator or innovation in March 2019, nothing came up on the USA Jobs website [39]. The government hiring process is long and cumbersome [40]. The "normal" plan for hiring someone required 81 days from the identification of a need to a person starting a position to fill that need [40]. Although OPM states some government departments may be faster, 81 days as a planning factor to hire a DoD employee seems to be enough time to screen for innovation. Traits of innovators described above could be screened for during the 81-day hiring time frame.

Two organizations within DoD are working around the normal hiring process in order to land innovative talent: the Defense Innovation Unit (DIU) and the Strategic Capabilities Office (SCO) [41]. DIU and SCO were given permission from Deputy Secretary of Defense in 2017 to hire needed expertise on 18-month noncompetitive contracts [42]. This permission allowed DIU and SCO to circumvent the onerous federal hiring process to quickly land the talent necessary in an organization designed to innovate.

It would seem that private sector hiring would be shorter, but the timelines between DoD and the commercial sector are similar. In the commercial sector, the hiring for what would be considered innovative jobs often takes many weeks to months [43], [42]. This is important to acknowledge because there is enough time in the hiring process to screen for innovation and screen against insider threat traits.

Currently, DoD is working to make itself an innovative organization with organizations like the Defense Innovation Board, The Defense Innovation Initiative and the Defense Innovation Marketplace. Unfortunately, within DoD there is not a formal effort outside of DIU to recruit innovators. The standard industrial age personnel practices are the norm and there is an obvious inadequacy of DoD recruitment of innovative personnel [3].

It may be useful to explore how innovators who might become malicious insiders might be identified. Although a full assessment of current DoD innovation recruitment is beyond the scope of this thesis, at the organizational level the research supports two conclusions. First, the DoD can and should foster the kind of organizational culture and environment that would nurture innovative skills and build the kind of organizational loyalty that innovative personnel want, which will also help identify and thwart insider threats. Second, an appropriately enhanced screening for the few personality traits of some innovators that may signal insider threat potential should not impede the speed or efficiency of bringing innovative talent into the DoD. The thesis conclusion builds on this second point.

# V. CONCLUSION

## A. OVERALL CONCLUSIONS

There is no overlap between the traits in malicious insider threats and innovators--in fact they seem to be wholly opposite unless there is an extreme ideological motivator involved, e.g., Klaus Fuchs. The closest convergence of innovator traits (insensitive, questioning attitude, abrasive) are with the three malicious insider threat traits (psychopathy, rebellious, passive aggressive).

Personality traits that lead to destructive behavior appear to be one of the keys to identifying DoD personnel who could be potential insider threats. Various personality instruments currently in use by psychologists [25] can tease out malicious insider threat personality traits. The ability to identify risk-taking behavior could aid in the identification of personnel with a propensity to become a UIT. Based on BART analysis, if a person is displaying risk-taking traits, then there should be supervisory controls in place to observe their behavior.

A biannual review may be insufficient to address the risk posed by a person who displays one or more UIT traits (careless, risk taking, disgruntled, mental health issues.) A quarterly (or more frequent) review may be warranted. This review may not be formal in nature, but a review of behavior in the workplace, e.g., are other insider threat traits being exhibited by the person demonstrating the UIT behavior; or is there a significant stressor in their life that could provide the motivation to become an insider threat.

Currently, cyber awareness computer-based training is likely the only formal training DoD employees receive about insider threats and solely focuses on the malicious insider. The UIT traits—"disgruntlement," "risk taker" and "carelessness"—are not specifically mentioned in DoD training. The only traits that get even close to disgruntlement are "persistent interpersonal difficulties" and "hostile vindictive behavior" [44]. Security clearance adjudication also does not screen for the UIT.

The following section builds on this point by taking a closer look at current DoD insider threat training and practices. The subsequent sections discuss other policy implications and opportunities to build further on the research of this thesis.

## B. DOD INSIDER THREAT TRAINING AND ADJUDICATION GUIDELINES

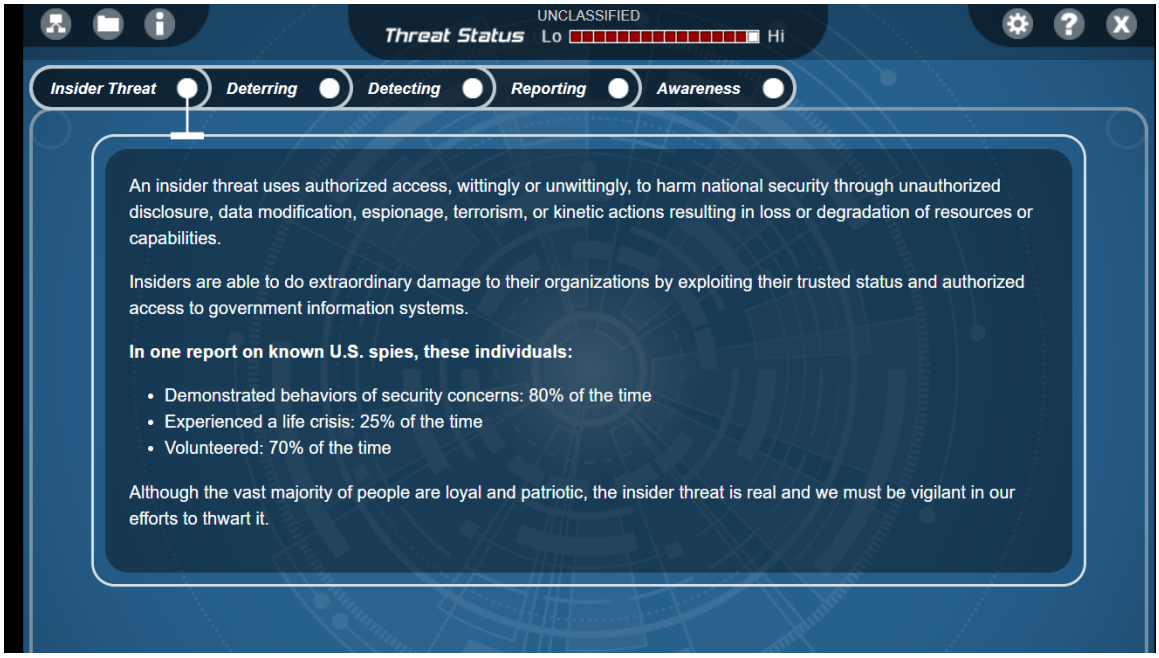
It is important to discuss both insider threat training within the DoD and the Adjudicative Guidelines for security clearance since they are both representative of the current insider threat trait understanding within the DoD. Additionally, capturing the current training and adjudication guidelines could help future insider threat research by providing a reference to what the training and guidelines were in 2019.

The literature on how and from what sources the DoD constructed its counter-intelligence training program is fairly sparse. There is one report by Fisher that a formalization in determining criteria for security clearances originated with the Stillwell Commission Report from 1985 [16]. The Stillwell Report was the driving factor behind the creation of the Defense Personnel Security Research Center (PERSEREC) in 1986 [16]. The Stillwell Report called for more scientific rigor when it came to determining why someone should be denied a security clearance. Of note, there is no formal test or investigation into the Dark Triad personality traits.

The traits used to conduct insider threat training for DoD uniformed and civilian employees are the same as the traits used to conduct security clearance background check adjudications for all government employees requiring access to classified information [44], [45]. The training also tangentially refers to the two indicators of UIT, mental health issues and disgruntlement, but neglects risk taking and carelessness. Insider threat training should have more emphasis on the UIT.

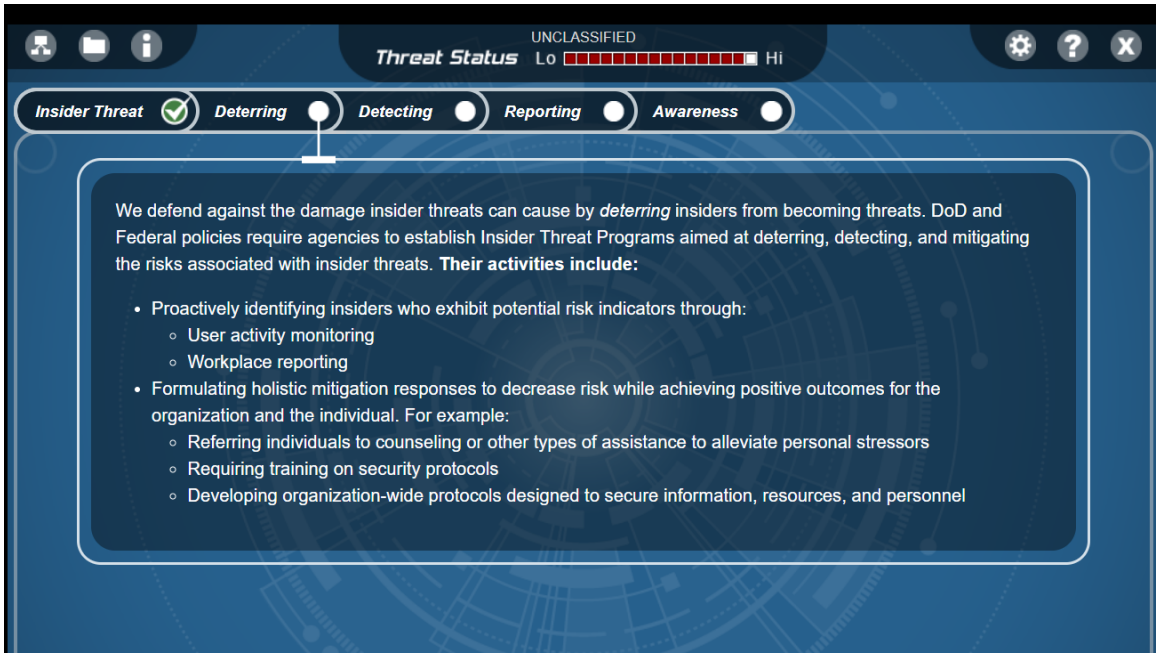
Figures 3–6 are from the 2019 U.S. Government Cyber Awareness Training that is the training for DoD employees. Although not traits but behavioral indicators, it is important to note the current state of training because that is the ground truth for the DoD employees' understanding of insider threats. Unless insider threat research is part of their day-t- day job, most employees will not know any more about insider threat than what this training provides.

Figure 3. Insider Threat Training—Definition and Facts. Adapted from [44].



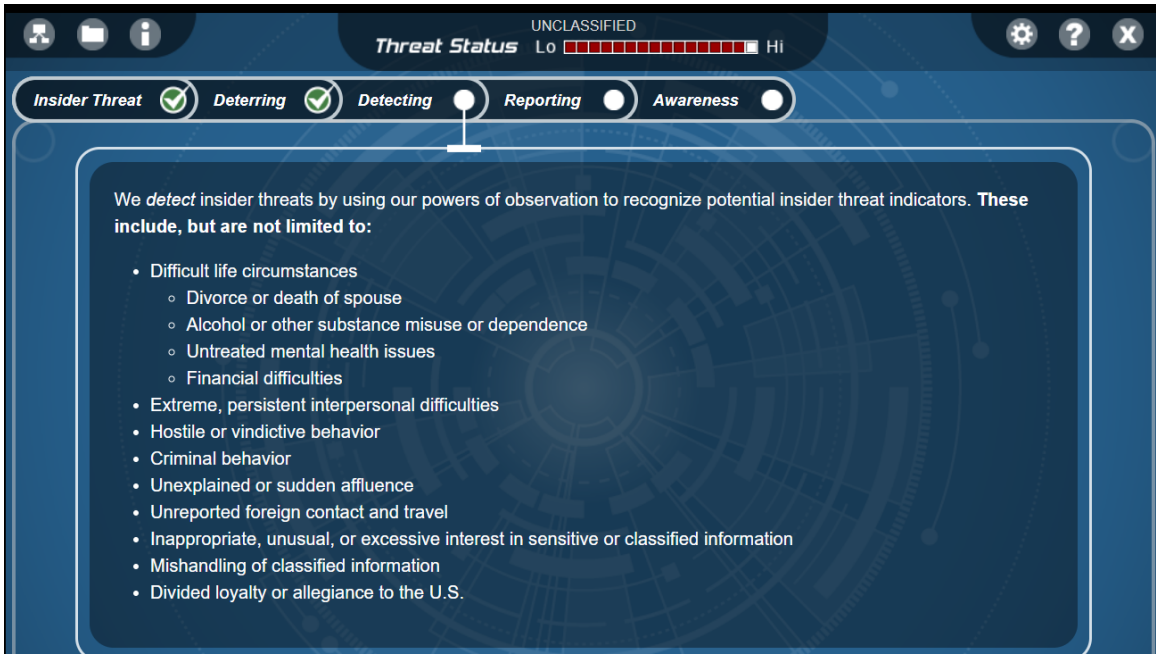

The above Computer-Based training is currently what DoD employees receive. Herbig reports life crisis is experienced 33% of the time vice the training number of 25%. The training does not cite the source [46].

Figure 4. Insider Threat Training—Deterrence. Adapted from [44].



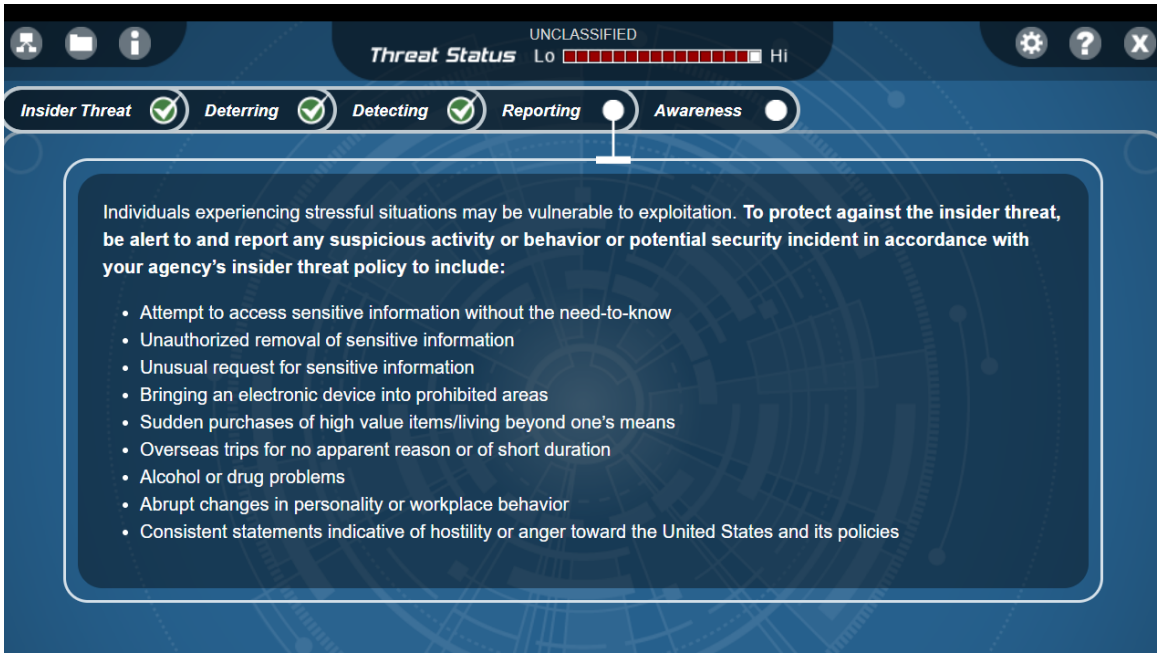

The insider threat training does focus on both technical (user monitoring) and behavior indicators (workplace reporting).

Figure 5. Insider Threat Training—Detection. Adapted from [44].




Detecting insider threat portion of the training focuses on many of the insider threat traits in the literature.

Figure 6. Insider Threat Training—Reporting. Adapted from [44].




The reporting module expands on the detection module; there are additional malicious insider threat traits evident in the reporting module of the training.

The Security Executive Agent Directive 4 lays out the criteria used to evaluate a person for a sensitive position with access to classified information [45]. These guidelines are important to analyze because they represent DoD understanding and implementation of insider threat risk. The adjudicative guidelines are currently the only instrument in DoD used to determine if an employee is potentially and insider threat and does not meet the standard for access to sensitive information. The criteria are:

> Allegiance to the U.S. – No involvement in espionage, treason, terrorism or sedition against the U.S.
>
> Foreign Influence – Connection to a foreign person or group that can create a potential conflict of interest
>
> Foreign Preference –Applying for citizenship in another country, entering the U.S. with foreign passport, acting to serve the interests of a foreign entity that conflicts with U.S. national security interests
>
> Sexual Behavior – A pattern of sexual behavior that is high risk, destructive. Sexual behavior that can be used for coercion or exploitation
>
> Personal conduct – Failure to exercise good judgment, lack of candor during the security interview process, dishonesty or unwillingness to comply with rules and regulations
>
> Financial Considerations – Failure to live within means, pay debts and meet financial obligations
>
> Alcohol Consumption- Excessive alcohol use results in failure to control impulses, exercise questionable judgment
>
> Drug Involvement- Illegal use or possession of controlled substances
>
> Psychological Conditions- An opinion by a duly qualified mental health professional that a condition may impair judgment, stability, reliability and trustworthiness. Pathological gambling.
>
> Criminal Conduct – Criminal activity displays individuals' lack of concern for rules and regulations
>
> Handling Protected Information- Deliberate or negligent failure to comply with rules and regulations when handling protected information
>
> Outside Activities- Involvement in employment or activities with a foreign entity that could pose a conflict of interest

Use of Information Technology- Unauthorized entry, modification, destruction or use of information technology. [45]

The above guidelines do not appear comprehensive enough to cover the MIT and UIT traits. Risk taker, carelessness, and disgruntlement appear in almost every aspect of malicious and unintentional insider threat traits (Figure 2) and should be specifically called out in the adjudicative guidelines. The only outliers are the use of information technology and risk propensity.

The influence of foreign persons, governments and entities is woven throughout the National Security Adjudicative Guidelines [45]. The insider threat trait most closely associated with foreign influence is the reduced loyalty trait [30]. As loyalty to the U.S. becomes less of an influence on a malicious insider, then they could have more of a propensity to be influenced by a foreign government.

## C. POLICY IMPLICATIONS

There is a clear need for DoD to recruit innovative personnel. Currently, there is not a concerted effort to recruit innovators outside of the DIU [3], [39]. Even if there was a concerted effort to recruit innovative personnel, the processes are not in place within DoD to foster innovation [3]. Innovation within DoD will require a revolutionary overhaul of policy [3], especially in system acquisitions, the ability to move money [3], and personnel hiring [3] and firing policies. Along with the recruitment of innovators, fostering a more innovative culture is of the utmost importance in the current age of global cyber operations. Ensuring that innovators do not have a propensity to be an insider threat is critically important. This thesis has shown that innovators are not more of an insider threat; in fact, many characteristics of innovators are the opposite of those of an insider threat.

The current state of background investigations may already be insufficient to take into account personality traits of potential insider threats. Thus, enhancing background investigations to account for the few innovator traits that may also indicate insider threat potential is an opportunity to improve the background investigation process more generally. The traits of insensitivity, abrasiveness and rebelliousness also deserve more

careful scrutiny in efforts to thwart malicious insider threats. Most importantly, investigations should focus on the one trait that the UIT and innovator share together: risk taking.

Furthermore, mental health issues and disgruntlement are two traits shared by UIT and malicious insiders. The DoD should screen personnel for risk taking trait with the Balloon Analogue Risk Task (BART). Finally, the DoD should continue to screen for mental health issues and first line supervisors should intervene quickly to help a disgruntled employee assuage the issues at the root cause of their disgruntlement.

## D. RECOMMENDATIONS FOR FUTURE WORK

The Dark Triad personality traits need to be researched further with regard to the insider threat, especially narcissism. Current DoD training and security clearance adjudication guidelines do not touch on the narcissistic personality type. Machiavellianism (deception) and psychopathy (erratic behavior) are touched upon in the training and clearance adjudication guidelines. The only innovator traits that overlap with UIT is risk taking, "individuals engaging in behavior and activities without intent to cause harm to the organization may also be the same individuals that eventually do seek to engage in activities with malicious intent" [19]. Future work could include DoD research on the use of current personality tests to determine risk-taking propensity.

Although outside the scope of this thesis, future work should examine whether and how ideology coupled with innovation may produce an insider threat. Additionally, further research should be done on why the Department of Treasury definition and insider threat policy is so different from the other departments studied in this thesis.

THIS PAGE INTENTIONALLY LEFT BLANK

# LIST OF REFERENCES


[1] Verizon, "2018 Data Breach Investigations Report (DBIR)," no. 11, *Verizon Bus. J.*, 2018.

[2] S. Kipp, "Espionage and the Insider," *Inf. Secur.*, p. 18, 2003.

[3] E. Schmidt, "Statement of Dr. Eric Schmidt House Armed Services Committee," 2017. [Online] Available: https://docs.house.gov/meetings/AS/AS00/20180417/108132/HHRG-115-AS00-Wstate-SchmidtE-20180417.pdf.

[4] *Department of Defense Directive 4180.01*, no. 5205, pp. 1–16, 2014., Office of the Under Secretary of Defense for Acquisition Technology and Logistics, Washington, DC, USA, 2014.

[5] CERT/ Insider Threat Team, "Unintentional Insider Threats : A Foundational Study. (CMU/SEI-2013-TN-022)," 2013.

[6] Department of Homeland Security, "Insider threat," 2018. [Online]. Available: https://www.dhs.gov/science-and-technology/csd-insider-threat.

[7] Order, Department of Energy, DOE O 470.5, U.S Department of Energy, Washington, DC, USA, 2014.

[8] Order, Department of the Treasury, DOT 105–20, U.S. Department of Treasury, Washingtion, DC, USA, 2013. [Online]. Available: https://www.treasury.gov/about/role-of-treasury/orders-directives/Pages/to105-20.aspx

[9] National Insider Threat Task Force, "Insider Threat Program Maturity Framework," Washington, DC, 2018. [Online]. Available: https://www.dni.gov/files/NCSC/documents/nittf/20181024_NITTF_MaturityFramework_web.pdf

[10] M. Kirton, "Adaptors and Innovators: A Descritpion and Measure," *J. Appl. Psychol.*, vol. 61, no. 5, pp. 622–629, 1976.

[11] "Innovator." *Oxford Dictionary*. Accessed February 21, 2019. [Online]. Available: https://en.oxforddictionaries.com/.

[12] H. Olander, M. Vanhala, P. Hurmelinna-Laukkanen, and K. Blomqvist, "Preserving prerequisites for innovation," *Balt. J. Manag.*, vol. 11, no. 4, pp. 493–515, 2016.

[13] S. Wood and M. F. Wiskoff. “Americans who spied since WWII,” PERSEREC, Monterey, CA, Rep. PERS-TR-92-005, 1992.

[14] M. F. Wiskoff and K. L. Herbig, “Espionage against U.S. 1947–2001,” PERSEREC, Monterey, CA, Rep. TR-02-5, 2002.

[15] Intelligence Community Staff, “Project Slammer Interim progress report.” Washington, DC, Rep. ICS 0858–90, 1990. [Online]. Available: https://www.cia.gov/library/readingroom/docs/DOC_0000218679.pdf

[16] L. F. Fischer, “Espionage : Why does it happen ?,” 2000. [Online]. Available: https://www.hanford.gov/files.cfm/whyhappens.pdf

[17] Department of Defense USA, “DoD insider threat mitigation - final report of the Insider Threat Integrated Process Team,” Falls Church, VA, 2000. [Online]. Available: http://www.dtic.mil/dtic/tr/fulltext/u2/a391380.pdf

[18] M. Maasberg, J. Warren, and N. L. Beebe, “The dark side of the insider: detecting the insider threat through examination of dark triad personality traits,” *Proc. Annu. Hawaii Int. Conf. Syst. Sci.*, vol. 2015-March, pp. 3518–3526, 2015. [Online]. doi: 10.1109/HICSS.2015.423

[19] M. Dupuis and S. Khadeer, “Curiosity killed the organization: A psychological comparison between malicious and non-malicious insiders and the insider threat,” *Proc. 5th Annu. Conf. Res. Inf. Technol.*, pp. 35–40, 2016. [Online]. doi: 10.1145/2978178.2978185

[20] A. Vashisth and A. Kumar, “Corporate espionage: the insider threat,” *Bus. Inf. Rev.*, vol. 30, no. 2, pp. 83–90, 2013. [Online]. doi: 10.1177/0266382113491816

[21] S. J. Stolfo and Bowne, “Insider threat defense,” in *Encyclopedia of Cryptography and Security*, H. Van Tilborg and S. Jajodia, Eds. 2011, pp. 609–611.

[22] F. Farahmand and E. H. Spafford, “Understanding insiders: An analysis of risk-taking behavior,” *Inf. Syst. Front.*, vol. 15, no. 1, pp. 5–15, 2013. [Online]. doi: 10.1007/s10796-010-9265-x

[23] A. Tversky and D. Kahneman, “Judgment under uncertainty : Heuristics and biases.” linked references are available on JSTOR for this article : Judgment under Uncertainty : Heuristics and Biases,” *Science (80-. ).*, vol. 185, no. 4157, pp. 1124–1131, 1974. [Online]. doi: 10.1126/science.185.4157.1124

[24] M. Kirk, *The Man Who Knew*. PBS, 2002. [Online]. Available: https://www.pbs.org/video/frontline-the-man-who-knew/

[25] F. L. Greitzer *et al.*, “Unintentional insider threat: Contributing factors, observables, and mitigation strategies,” *Proc. Annu. Hawaii Int. Conf. Syst. Sci.*, pp. 2025–2034, 2014. [Online]. doi: 10.1109/HICSS.2014.256

[26] P. A. Epstein, “Tesla stock plummets after Elon Musk smokes weed on live show and two execs quit in one day,” *NBC News.com*, 2018. [Online]. Available: https://www.nbcnews.com/tech/tech-news/tesla-stock-plummets-after-elon-musk-smokes-weed-live-show-n907476

[27] R. Agarwal and J. Prasad, “A conceptual and operational definition of information technology,” *Inf. Syst. Res.*, vol. 9, no. 2, pp. 204–215, 1998. [Online]. doi: 10.1287/isre.9.2.204

[28] E. Velasco, I. Zamanillo, and T. Garcia Del Valle, “Mobilizing company members’ full innovative potential,” *Hum. Factors Ergon. Manuf.*, no. 6, pp. 541–559, 2012. [Online]. doi: 10.1002/hfm

[29] B. Sandberg, L. Hurmerinta, and P. Zettinig, “Highly innovative and extremely entrepreneurial individuals: What are these rare birds made of?,” *Eur. J. Innov. Manag.*, vol. 16, no. 2, pp. 227–242, 2013. [Online]. doi: 10.1108/14601061311324557

[30] N. (Peter) Liang, D. P. Biros, and A. Luse, “An empirical validation of malicious insider characteristics,” *J. Manag. Inf. Syst.*, vol. 33, no. 2, pp. 361–392, 2016. [Online]. doi: 10.1080/07421222.2016.1205925

[31] W. Isaacson, *The Innovators*. New York, NY: Simon and Shuster, 2014

[32] K. Smith and L. Richardson, “Measuring innovation,” in *Brand Strategy*, no. 166, 2002, p. 3. [Online]. doi: 10.1093/oxfordhb/9780199286805.003.0006

[33] S. G. Scott and R. A. Bruce, “Determinants of innovative behavior- A path model of individual innovation in the workplace,” *Acad. Manag. J.*, vol. 37, pp. 580–607, 1994. [Online]. doi: 10.1007/978-3-211-79271-1_2

[34] K. Hölzle, M. N. Mansfield, and H. G. Gemünden, “Personal characteristics of innovators — an empirical study of roles in innovation management,” *Int. J. Innov. Manag.*, vol. 14, no. 06, pp. 1129–1147, 2010. [Online]. doi: 10.1142/s1363919610003033

[35] M. A. Schilling, *Quirky*. New York, NY: PublicAffairs Hachette Book Group, 2018.

[36] K. Hafner and M. Lyon, *Where Wizards Stay Up Late*. New York, NY: Touchstone, 1996.

[37] C. Timberg, “Net of insecurity part one: A flaw in the design,” *The Washington Post*, 30-May-2015. [Online]. Available: https://www.washingtonpost.com/sf/business/2015/05/30/net-of-insecurity-part-1/?utm_term=.002358d5e7fa

[38] United States House of Representatives, “Review of the unauthorized disclosures of former national security agency contractor Edward Snowden,” 2016. Washington, DC, [Online]. Available: https://www.hsdl.org/?abstract&did=797546

[39] U.S. Government, “USA Jobs,” 2019. [Online]. Available: https://www.usajobs.gov/Search/?k=innovator%2C innovation

[40] OPM, “Office of Personnel Management,” 2019. [Online]. Available: https://www.opm.gov/policy-data-oversight/human-capital-management/hiring-reform/hiring-process-analysis-tool/enter-on-duty/

[41] M. Aaron, “Defense News,” 2017. [Online]. Available: https://www.defensenews.com/pentagon/2017/08/10/diux-sco-given-special-hiring-and-contracting-authorities/.

[42] Job Message Board, “Indeed,” 2019. [Online]. Available: https://www.indeed.com/cmp/Amazon.com/faq/how-long-does-it-take-to-get-a-start-date?quid=1ae82m5i50kbp7qg

[43] B. See, “Forbes,” 2015. [Online]. Available: https://www.forbes.com/sites/quora/2015/01/09/why-does-google-recruiting-take-so-long/#3efb86d53fc4

[44] U.S. Government, “Cyber awareness challenge for the intelligence community DS-IA110.06,” 2109. [Online]. Available: https://cdse.usalearning.gov/

[45] Office of Director of National Intelligence, “Securtiy executive agent directive 4: national security ajudicative guidelines,” Washington, DC, 2017. [Online]. Available: http://ogc.osd.mil/doha/SEAD4_20170608.pdf

[46] K. L. Herbig, “Changes in espionage by Americans: 1947–2007,” Monterey, CA, PERSEREC Technical Report No. 08–05, 2008.

# INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California