PERSEREC

OPA Report No. 2019-067
PERSEREC-TR-19-05

October 2019

An Evaluation of the Utility of Expanding Psychological Screening to Prevent Insider Attacks

Jessica A. Baweja
Shannen M. McGrath
Northrop Grumman Technology Services

Danielle Burchett
TechWerks

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

OPA
OFFICE OF PEOPLE ANALYTICS

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

OPA Report No. 2019-067 **PERSEREC-TR-19-05** **October 2019**

An Evaluation of the Utility of Expanding Psychological Screening to Prevent Insider Attacks

Jessica A. Baweja & Shannen M. McGrath
Northrop Grumman Technology Services

Danielle Burchett
TechWerks

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

Released by – Eric L. Lang

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

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

1. REPORT DATE:	2. REPORT TYPE: Technical Report	3. DATES COVERED:
4. TITLE: An Evaluation of the Utility of Expanding Psychological Screening to Prevent Insider Attacks	5a. CONTRACT NUMBER:	
	5b. GRANT NUMBER:	
	5c. PROGRAM ELEMENT NUMBER:	
6. AUTHOR(S): Jessica A. Baweja, Shannen M. McGrath, Danielle Burchett, & Stephanie L. Jaros	5d. PROJECT NUMBER:	
	5e. TASK NUMBER:	
	5f. WORK UNIT NUMBER:	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES): Defense Personnel and Security Research Center Office of People Analytics 400 Gigling Road Seaside, CA 93955	8. PERFORMING ORGANIZATION REPORT NUMBER PERSEREC: There are two report numbers: PERSEREC-TR-19-05 OPA Report No. 2019-067	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES):	10. SPONSORING/MONITOR'S ACRONYM(S):	
	11. SPONSORING/MONITOR'S REPORT NUMBER(S):	
12. DISTRIBUTION/AVAILABILITY STATEMENT: A		
13. SUPPLEMENTARY NOTES:		

ABSTRACT: The Office of the Under Secretary of Defense for Intelligence funded the Defense Personnel and Security Research Center to assess whether expanding psychological screening to include all DoD applicants could prevent future insider attacks. In furtherance of this goal, researchers conducted a literature review and interviewed subject matter experts (SME) in psychological assessment, screening, and insider threat. Overall, although the literature and SMEs suggested that individual predispositions (*i.e.*, personality traits, emotional issues, social skills deficits, and mental health symptoms and diagnoses) are relevant to the risk of insider attacks, and several organizations model effective screening programs, findings here suggest that large-scale implementation of psychological screening for DoD applicants is premature due to a number of considerations. First, psychological assessment of relevant personality and mental health characteristics requires significant expertise, time, money, and labor to administer effectively. Second, due to the high-stakes context, it is likely that applicants will misrepresent their responses. The authors recommend that any expansion of psychological screening in DoD should focus only on the highest risk groups, and any screening process should include an assessment of response validity to account for deception. DoD also should carefully consider the side effects of additional screening on the future applicant and current employee populations prior to any significant expansion.

14. SUBJECT TERMS: insider threat, social and behavioral science, psychology, psychological screening, vetting

15. SECURITY CLASSIFICATION OF: Unclassified			16. LIMITATION OF ABSTRACT:	17. NUMBER OF PAGES: 39	19a. NAME OF RESPONSIBLE PERSON: Eric L. Lang, Director
a. REPORT:	b. ABSTRACT:	c. THIS PAGE:			19b. TELEPHONE NUMBER (Include area code): 831-583-2846

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

PREFACE

Shaw and Sellers' (2015) Critical Pathway Model (CPM) has emerged as a leading framework to conceptualize the transformation of a trusted insider into a malicious attacker. CPM, however, is a descriptive framework rather than a predictive model, which limits its utility for policymakers. This report assesses the empirical evidence that underlies one portion of the CPM—individual predispositions—to determine whether or not DoD should expand its psychological screening program to include more, if not all, applicants as one way to fairly, efficiently, and effectively mitigate the risk of future insider attacks.

Eric L. Lang
Director, PERSEREC

EXECUTIVE SUMMARY

The Critical Pathway Model (CPM) describes a person's transition from an insider to an insider threat as the outcome of a combination of individual predispositions, stressors, concerning behaviors, and organizational vulnerabilities (Shaw & Sellers, 2015). One potential application of the CPM within the Department of Defense (DoD) is to screen applicants for those individual predispositions as part of the vetting process.

The Office of the Under Secretary of Defense for Intelligence funded the Defense Personnel and Security Research Center to evaluate whether DoD should expand psychological screening to include more, if not all, applicants (*i.e.*, military, civilian, and contractor) as part of its multi-layered strategy to prevent insider attacks. The research questions are as follows:

- What empirical evidence supports the CPM's association between individual predispositions and insider attacks? How strong is this evidence?
- How do organizations currently use psychological screening to identify individual predispositions that may compromise their mission?
- What best practices and lessons learned should DoD consider from organizations that currently use psychological screening?

METHOD

This study included a review of the unclassified literature and interviews with subject matter experts (SME) with expertise in the administration and/or development of psychological assessments. Telephone interviews with nine SMEs were completed and field notes were taken to capture the main ideas. Questions focused on predispositions related to insider threat, current assessment practices, and lessons learned for DoD to consider related to psychological screening. The field notes were analyzed for patterns and the most common themes were incorporated into the results, findings, and recommendations.

RESULTS

Individual Predispositions & Insider Attacks

Based upon patterns identified in both the unclassified literature review and SME interviews, individual predispositions can be organized into the following categories: (1) personality traits, (2) emotional issues and social skills deficits, and (3) mental health symptoms and diagnoses. First, the Dark Triad set of traits includes narcissism, psychopathy, and Machiavellianism, and appears in a number of studies related to insider attacks. The Dark Triad personality traits describe individuals who are manipulative, self-centered, and lack empathy for others, and, therefore, may present a higher risk of insider attack (Maasberg, Warren, & Beebe, 2015; Paulhus & Williams, 2002; Wilder, 2017). Also, a number of researchers have noted the relevance of Big Five personality traits to insider attacks. For example, low levels of extraversion and agreeableness are related to the risk of insider attack (Shaw *et al.*, 1998; Salgado, 2002).

Second, research suggests that a tendency toward frustration, anger, and disgruntlement increases the risk of insider attack (*e.g.*, Shaw, Ruby, & Post, 1998). Deficient social skills, which can create difficulties working with others, also may present a risk (*e.g.*, Shaw & Stock, 2011). Third, certain mental health issues (*e.g.*, psychosis) may relate to an increased risk of insider attack (*e.g.*, Shaw & Sellers, 2015).

Psychological Screening in Practice

In contrast with many municipal and state law enforcement and public safety agencies, few organizations in the Federal Government use psychological screening for all applicants. One of the few exceptions, the Department of Energy's Human Reliability Program, requires applicants and employees to undergo in-depth psychological assessment, including a semi-structured interview, mental status exam, cognitive testing, and self-reported psychopathology testing. In general, organizations that use psychological screening ask applicants to complete a psychological assessment and use responses either to screen applicants out of candidacy or select them for more comprehensive screening.

Best Practices & Lessons Learned

Three themes emerged for DoD to consider with regard to psychological screening. First, psychological assessments require significant resources and, thus, are expensive. Psychological assessments also present an opportunity for applicants to misrepresent themselves in an effort to get hired, which must be accounted for in screening programs (*e.g.*, Levashina, 2018). Finally, screening programs may have consequences (*e.g.*, decreased morale or recruitment), so organizations should consider the benefits relative to risk prior to implementation (*e.g.*, Shaw, Fischer, & Rose, 2009).

FINDINGS & RECOMMENDATIONS

Finding #1: Although there is solid evidence that individual predispositions are related to the risk of insider attacks, additional research is required prior to large-scale implementation of psychological screening in DoD.

- **Recommendation #1a**: DoD should explore the links among personality dysfunction, psychopathology assessments, and pre-attack behaviors, such as counterproductive workplace behaviors, which occur at a greater frequency than insider attacks. Such a study could help to identify the incremental utility of using well-established tools in multiple domains (*e.g.*, MMPI, Dark Triad, Big Five) and also identify the level at which different personality traits may relate to problematic behaviors, including concerns associated with insider attacks.

- **Recommendation #1b:** DoD should review the classified literature on individual predispositions and insider attacks. SME discussions suggested that there are some approaches within the classified domain that may provide useful information for DoD's Counter Insider Threat Program, but further research is necessary to understand those processes and their value.

Finding #2: All SMEs consulted for this effort suggested DoD should expand psychological screening to include more, *but not all*, applicants.

- **Recommendation #2a**: Screening every applicant is not feasible. Instead, screening should focus first on individuals who present the highest risk due to job position (*e.g.*, seniority or access to sensitive information) and DoD should further triage based on the results of an assessment process to identify even smaller groups of individuals for more extensive psychological evaluation.

- **Recommendation #2b:** Psychological assessments only at the time of application are insufficient, as individual risk changes over time. Organizations across DoD also should use psychological screening to assess employees for cause (*e.g.*, reports from co-workers, supervisors) during the course of their careers.

Finding #3: Psychological screening must consider the likely possibility that applicants will misrepresent themselves.

- **Recommendation #3a**: Screening programs should include tools with well-validated embedded validity scales to address concerns of applicant deception (*e.g.*, PAI, MMPI-2, MMPI-2-RF).

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ACRONYMS USED IN THIS REPORT

CERT	National Insider Threat Center, CERT Division, Software Engineering Institute
CPM	Critical Pathway Model
CWB	Counterproductive Workplace Behavior
DIRE	Dispositional Indicators of Risk Exposure
DOE	Department of Energy
HEXACO	Humility-Honesty, Emotionality, Extraversion, Agreeableness, Conscientiousness, and Openness to Experience
IPI	Inwald Personality Inventory
IT	Information Technology
LBQ	Lackland Behavioral Questionnaire
MMPI	Minnesota Multiphasic Personality Inventory
MMPI-2	Minnesota Multiphasic Personality Inventory—2
MMPI-2-RF	Minnesota Multiphasic Personality Inventory—2 Restructured Form
PAI	Personality Assessment Inventory
PERSEREC	Defense Personnel and Security Research Center
SF-86	Standard Form 86, *Questionnaire for National Security Positions*
SME	Subject Matter Expert
SWAP	Shedler-Westen Assessment Procedure
USSS	United States Secret Service

INTRODUCTION

Insiders are individuals with authorized access to an organization's information, facilities, networks, resources, and people. Insiders who go on to harm their organizations become insider threats. The Critical Pathway Model (CPM) has emerged as a leading framework to describe this transition from a trusted insider to an insider threat by way of a combination of individual predispositions (*e.g.*, psychiatric conditions, personality dysfunction, social skills deficits), personal stressors, concerning behaviors, and organizational vulnerabilities (Shaw *et al.*, 1998; Shaw & Sellers, 2015). These four elements are largely chronological, and their interaction over time creates the possibility of an insider attack, as illustrated in Figure 1.

Figure 1 The Critical Pathway

Excerpted from Jaros, 2017; adapted from Shaw & Sellers, 2015

Because of its popularity and accessibility, DoD is interested in fair and effective ways to operationalize the CPM to improve its Counter Insider Threat Program. One such effort focuses on the individual predispositions that may increase the risk of future insider attacks, and whether expanding the use of psychological screening to include more, if not all applicants could decrease such risk.

Such an application, however, has both challenges and limitations. For example, studies that include psychological data associated with any kind of insider threat behavior are rare. Moreover, the studies that do exist often are based on retrospective assessment data, which makes it challenging to systematically assess which individual predispositions are most relevant to the small subset of malicious, intentional insider attacks (Band *et al.*, 2006; Noonan, 2018). Finally, much of the relevant research derives from individual case studies, which, by their nature, do not generalize to the larger population.

Even more broadly, although individual predispositions are part of the foundation to conceptualize insider risk, "only a small minority of persons with these characteristics or experiences goes on to commit insider actions, and only after they have been exposed to additional stressors on the critical path" (Shaw & Sellers, 2015: p.44). Thus, the Office of

the Under Secretary of Defense for Intelligence (OUSD[I]) funded the Defense Personnel and Security Research Center (PERSEREC), a division of the Office of People Analytics, to assess whether expanding psychological screening to include most, if not all DoD applicants would be a fair, effective, and efficient tool to prevent insider threats.

CURRENT STUDY

This study combines an unclassified literature review with subject matter expert (SME) interviews to evaluate the association between individual predispositions and insider threat attacks. Per OUSD(I)'s request, this effort focuses primarily on intentional insider threat behavior (hereinafter, "insider attacks") rather than on unintentional behaviors, such as mistakes, inattention, or negligence. The information from this study will help to determine whether psychological screening should be expanded to include most, if not all DoD applicants as a way to mitigate future risk. The research questions are as follows:

- What empirical evidence supports the CPM's association between individual predispositions and insider attacks? How strong is this evidence?
- How do organizations currently use psychological screening to identify individual predispositions that may compromise their mission?
- What best practices and lessons learned should DoD consider from organizations that currently use psychological screening?

METHOD

This study involved a comprehensive review of the unclassified literature and a series of SME interviews to understand how psychological assessments are used currently in DoD and in other organizations, along with both the benefits and limitations of various applications. What follows is a description of the literature review and interview design, execution, and data analysis processes.

LITERATURE REVIEW

Three trained researchers identified unclassified, publicly-available citations related to insider threat predispositions and psychological assessment practices in both government and open-access databases. Detailed notes of each article were recorded, organized by research question, and synthesized into a summary of the literature.

INTERVIEWS

Participants were recruited for this study because they were well-known experts in the administration and/or development of psychological assessments. Nine SMEs were interviewed from nine different organizations that use or conduct research in psychological screening, one within DoD and the remaining eight from other Federal Government agencies. One individual from the Intelligence Community was interviewed. Eight SMEs were clinical psychologists and one was a social-personality psychologist.

Telephone interviews were conducted between December 2018 and April 2019 using a semi-structured instrument that included open-ended questions related to possible precursors of insider threat behavior, the design and administration of psychological assessments, and costs versus benefits of psychological screening. Two or more members of the research team attended each interview except for one, which was staffed by a single interviewer due to scheduling conflicts.

Detailed field notes were taken and returned to SMEs for review, revision, and approval. Six SMEs provided feedback and approved a final version of field notes. Three SMEs did not respond to requests for feedback and were informed after a period of no less than 2 weeks that the version of the field notes they received would be considered final. Following completion of the interviews, field notes were analyzed for common themes and integrated into the results of the literature review to construct the results and recommendations that follow.

RESULTS

The results that follow are based on the unclassified literature and SME interviews. Results begin with a description of the individual predispositions relevant to insider attacks followed by a summary of psychological screening procedures in place within select organizations. The final section presents the best practices and lessons learned from the literature and SME interviews for DoD to consider as part of the decision to expand psychological screening to include more applicants.

INDIVIDUAL PREDISPOSITIONS & INSIDER ATTACKS

Given this project's ultimate aim to address the potential benefit of expanded psychological screening, results focus on individual predispositions related to habitual patterns of thought, behavior, or mental health symptoms or diagnoses; external factors such as social networks are outside the scope of this study. Based upon patterns identified in both the literature review and SME interviews, predispositions are organized into the following categories: (a) personality traits, (b) emotional issues and social skills deficits, and (c) mental health symptoms and diagnoses. For additional information, Appendix A summarizes the case studies that identified these predispositions, and Appendix B presents detailed information, including citations, for each of the specific individual predispositions.

Personality Traits

Both the unclassified literature and SME interviews highlighted two well-established personality trait models associated with counterproductive workplace behavior (CWB), including insider attacks. These two models–The Dark Triad and The Big Five–are summarized in the sections that follow.

The Dark Triad

The Dark Triad, which includes narcissism, psychopathy, and Machiavellianism, appears in a number of studies related to insider attacks (Jakobwitz & Egan, 2006; Paulhus & Williams, 2002). Figure 2 lists each trait with a sample of corresponding descriptors.

Narcissism	Psychopathy	Machiavellianism
•*Egocentric* •*Entitled* •*Vain* •*Sensitive to criticism* •*Grandiose* •*Requires admiration and recognition* •*Envious*	•*Impulsive* •*Thrill-seeking* •*Low empathy* •*Low anxiety* •*Lacks meaningful relationships* •*Cruel* •*Disdainful*	•*Manipulative* •*Ambitious* •*Exploitative* •*Charming* •*Deceptive* •*Flattering* •*Socially adept*

Figure 2 The Dark Triad

Jakobwitz & Egan, 2006; Paulhus & Williams, 2002

Overall, individuals high in Dark Triad traits tend to be socially malevolent, aggressive or hostile in their orientation toward the world, and lack remorse or empathy (Paulhus & Williams, 2002). They also are more likely to display a negative attitude and to develop malicious intent. Therefore, given motive, opportunity, and capability, these people may be more likely to engage in CWB, deception, and insider attacks (Maasberg *et al.*, 2015).

Within the Dark Triad, narcissism is especially relevant to insider attacks. Individuals high in narcissism feel entitled to recognition and to success, and their egos are particularly fragile. These individuals maintain fantastic ideas about their own talents and capabilities, and they believe themselves to be above the rules and exempt from policies, which may put them at higher risk of becoming an insider threat (Band *et al.*, 2006; Wilder, 2017).

Some studies discuss the relevance of narcissism overall (Nurse *et al.*, 2014; Paulhus & Williams, 2002; Shaw & Sellers, 2015). Other studies refer to the importance of individual facets, or components, of narcissism, such as a sense of entitlement, either in addition to or without reference to the broader predisposition (Band *et al.*, 2006; Moore *et al.*, 2011; Shaw *et al.*, 1998; Shaw & Stock, 2011; Wilder, 2017). Most studies discuss the subclinical personality trait[1] of narcissism as sufficiently relevant, although narcissistic personality disorder also is relevant. For example, Godes and Lang (2009) consulted with experienced adjudicators and identified malignant narcissism—a type of narcissism that involves high levels of antisocial behavior, aggression, and sadism—as the personality disorder that posed the greatest risk to personnel security.

There is further evidence that the Dark Triad, and particularly psychopathy, predicts the propensity to engage in misconduct such as drug abuse, minor criminality, serious criminality, driving misbehavior, bullying/harassing, anti-authority behavior, and high-stakes lying (*i.e.*, lying with serious consequences; Azizli *et al.*, 2016; Bergerstrøm, Larmour, & Farrington, 2018; Hare & Neumann, 2005; Skeem & Cooke, 2010). Psychopathy is characterized by low empathy, remorselessness, and impulsivity, and also is relevant to insider attacks, particularly violence (Band *et al.*, 2006; Godes & Lang, 2009; Shaw & Sellers, 2015; Wilder, 2017). For example, Hare Psychopathy Checklist-Revised scores show good predictive validity for violence, especially when compared to factors such as demographic characteristics, criminal history, or personality disorder diagnoses (Hare, 2003; DeMatteo, Edens, & Hart, 2010). In fact, psychopathy demonstrates as good or better prediction of violent behavior than some violence risk measures (*e.g.*, the Sexual Violence Risk—20; Boer, Wilson, Gauthier, & Hart, 1997; DeMatteo *et al.*, 2010).

Finally, there is evidence that the manipulative self-centeredness associated with Machiavellianism relates to insider attacks (Nurse *et al.*, 2014; Shaw & Stock, 2011). These individuals may present as calm, manipulative, and greedy, in contrast to the more egotistical or hostile characteristics associated with narcissism or psychopathy. Individuals high in Machiavellianism are motivated by ambition as well as by job

[1] Subclinical levels of a trait, such as narcissism, mean that the person possesses some of the characteristics associated with narcissism, but does not necessarily meet criteria for the related psychiatric diagnosis of narcissistic personality disorder.

dissatisfaction (Shaw & Stock, 2011). As a result, they may engage in theft, for instance, as a way to develop a new product or business for themselves.

The Big Five

According to researchers, the Big Five model describes the most important aspects of personality (John & Srivastava, 1999; McCrae & Costa, 1987).[2] Figure 3 lists the Big Five traits along with descriptors associated with high levels of each trait.

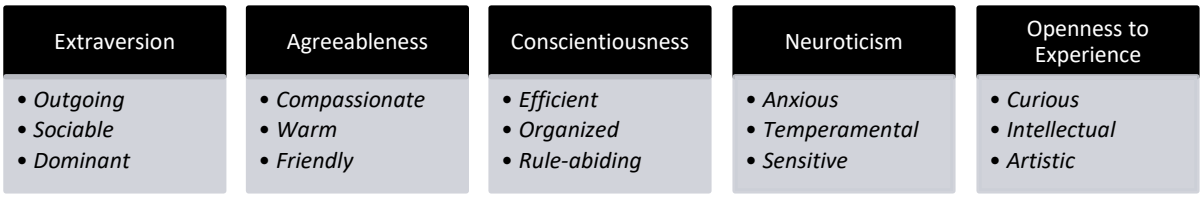

Figure 3 The Big Five Personality Traits

John & Srivastava, 1999; McCrae & Costa, 1987

A number of researchers have noted the relevance of Big Five personality traits to insider attacks. For example, low levels of extraversion and agreeableness are related to the risk of insider attacks (Shaw *et al.*, 1998; Salgado, 2002). Egan and Lewis (2011) linked aggression with The Big Five and found that high neuroticism predicted affective aggression (*i.e.*, angry, impulsive, or reactive aggressive behavior) while low agreeableness predicted both narcissistic (*i.e.*, ego-driven) and general (*i.e.*, generic) aggression.

Mount and colleagues (2006) explored how job satisfaction may mediate the association between Big Five traits and deviant behavior. Specifically, among customer service personnel, higher conscientiousness and agreeableness and lower neuroticism predicted lower workplace deviance. Job satisfaction partially mediated this association, particularly for agreeableness. In other words, job satisfaction at least partially explained the association between agreeableness and lower levels of workplace deviance (Mount, Iles, & Johnson, 2006).

Finally, other researchers have explored the links between CWBs and the HEXACO model of personality, which contains the Big Five traits plus the trait of honesty-humility (Ashton & Lee, 2007; Cohen, 2017). Previous research revealed that honesty-humility and conscientiousness predicted lower workplace deviance, higher organizational citizenship, and greater leadership effectiveness, which suggests a link between lower levels of honesty-humility and the risk of insider attacks (Cohen, 2017).

Emotional Issues and Social Skills Deficits

Beyond personality traits, researchers have identified emotional characteristics and social skills deficits relevant to insider attack. For example, a tendency toward frustration and

[2] It is worthwhile to note that some research has suggested that the Big Five might not generalize to non-Western cultures (*e.g.*, Laajaj *et al.*, 2019). Nonetheless, it remains the most commonly used model of personality traits.

anger as well as disgruntlement are consistently related to the risk of insider attack (Band *et al.*, 2006; Greitzer *et al.*, 2009; Greitzer, Kangas, Noonan, Dalton, & Hohimer, 2012; Liang, Biros, & Luse, 2016; Nurse *et al.*, 2014; Shaw *et al.*, 1998; Shaw & Fischer, 2005). One SME suggested that people who hold grudges and/or collect grievances also may pose a higher risk of insider attacks.

Deficient social skills also may increase the potential risk for insider attacks, particularly when they manifest as social isolation or an unwillingness or inability to interact capably with others (Band *et al.*, 2006; Shaw *et al.*, 1998; Shaw & Stock, 2011). When considered in combination with the previous emotional issues, these deficits and interpersonal problems provide a picture of a hostile, unpleasant, reactive individual who lacks the skills to respond adeptly to stress or to handle challenging social situations. Individuals who display these sorts of predispositions may, therefore, be at higher risk of committing an insider attack.

Mental Health Symptoms and Diagnoses

Overall, there is some evidence that certain mental health issues may confer an increased risk of insider attack. However, SMEs disagreed about the degree to which efforts should focus on assessment of psychopathology, or whether other predispositions may be of greater value. Nonetheless, research suggests certain diagnoses may be relevant to consider when screening for the risks associated with insider attacks.

Individuals with antisocial personality disorder are often aggressive, reckless, and callous, and they commonly engage in criminal behavior (Godes & Lang, 2009; Liang *et al.*, 2016; Skeem & Cooke, 2010). Additionally, avoidant personality disorder may lead to difficulties working and communicating with others, isolation, and potentially destructive behaviors (Liang *et al.*, 2016; Shaw & Sellers, 2015). Severe psychiatric conditions such as psychosis, bipolar disorder, and some personality disorders that are not well-controlled could create deficits that make an individual unstable, unreliable, or untrustworthy (Shaw & Sellers, 2015; Shechter & Lang, 2011).

Substance abuse issues also are of particular concern. Issues with substance abuse may increase a person's vulnerability toward insider threat behaviors, often through the stressors and challenges that tend to coexist with these issues, such as financial problems. That is, individuals who struggle with substance abuse may be at a higher risk of committing an insider attack, potentially as a way to alleviate issues related to their substance abuse (Band *et al.*, 2006; Nurse *et al.*, 2014; Shaw & Sellers, 2015).

PSYCHOLOGICAL SCREENING IN PRACTICE

Given the empirically supported associations between individual predispositions and concerning behavior, a number of organizations include psychological screening as part of their hiring process. As with other sections, the results that follow integrate information from the literature review and SME interviews; however, specific SME contributions are not necessarily highlighted to avoid identifying those who participated in this study.

At this time, the Federal Government does not psychologically assess all applicants, and the agency-specific assessments that are done on subsets of the population focus primarily on suitability for a particular position (*e.g.*, public safety positions, positions with access to special nuclear material) or to determine fitness for duty (*i.e.*, physically and psychologically fit to perform work functions).[3] This section presents examples of some of the different practices used across several Federal and non-Federal agencies.

Personnel who hold a position that requires eligibility to access sensitive or classified information undergo very limited mental health screening. In particular, applicants respond to Section 21 on the Standard Form 86 (SF-86), the *Questionnaire for National Security Positions*, which asks questions about mental health history. In response to a series of research studies, and in collaboration with a number of stakeholders, the Federal Government narrowed Section 21 in 2017 to focus specifically on the aspects of mental health found to be empirically related to safeguarding sensitive or classified information. Specifically, these aspects include having been diagnosed with certain psychiatric conditions (*i.e.*, psychotic disorders, bipolar disorder, borderline personality disorder, antisocial personality disorder) or having a history of psychiatric hospitalization or court-ordered mental health treatment (Shedler & Lang, 2015). If an applicant indicates such a mental health history on the SF-86, he/she may undergo additional psychological screening (Dickerhoof, Baweja, Osborn, & Smith, 2018).

In the Armed Forces, psychological screening is an important but non-uniform process. Currently, there is no standard Service-wide process to screen personality or psychopathology during the pre-accession process for military applicants (Cardona & Ritchie, 2006). Instead, existing Service-wide enlisted pre-accession screening efforts involve considering Armed Services Vocational Aptitude Battery and embedded Armed Forces Qualification Test aptitude scores in concert with a person's education level to inform job placement and overall qualification for entry. However, with first-term attrition at approximately 33%, and about 80% of those attritions due to behavioral problems or unsatisfactory performance, there is strong interest in preventing mental health attrition to reduce training costs and avoid exacerbating existing mental health problems (Cardona & Ritchie, 2006).

Some multi-stage efforts have been developed to screen large groups of Service members to identify higher-risk individuals for follow-up in-depth evaluation and services, and also to correct for screening measure coding errors (Cardona & Ritchie, 2006; Wright *et al.*, 2005; Wright, Huffman, Adler, & Castro, 2002). As one example, during U.S. Air Force basic military training, recruits complete the Lackland Behavioral Questionnaire (LBQ), a biographical data inventory (Garb, 2005). Results determine which recruits should undergo follow-up interviews with mental health technicians. A psychologist then reviews the results from both the LBQ and the interview, and then refers a sub-sample of recruits

[3] Although classified literature and processes are beyond the scope of this project, some agencies within the Intelligence Community require clinical screening of all applicants. Although details were not available in an unclassified conversation, one SME noted that all applicants must respond to a clinical assessment followed by a clinical interview.

to more intensive services (*e.g.*, emergency room for imminent risk, counseling for a remote history of suicidality, further evaluation for diagnostic considerations). This information also may be used to inform recommendations regarding who may be inappropriate for sensitive positions (Garb, Wood, & Baker, 2018).

To mitigate the risk of insider threats, all military, civilian, and contractor personnel who work within the scope of the DoD Nuclear Weapons Personnel Reliability Program are required to undergo initial certification evaluations as well as continuing evaluation to maintain certification (see DoDM 5210.42). Among the suitability factors considered are personal conduct (*e.g.*, questionable judgment, untrustworthiness, dishonesty, unwillingness to comply with rules), and psychological and personality disorders (*e.g.*, disorders that negatively affect judgment, reliability, or stability; high-risk, irresponsible, unstable, or aggressive behavior). Certifying professionals and competent medical authorities also are granted access to medical, mental health, police, and employment records for initial and continuous evaluation.

Similarly, the Department of Energy's (DOE) Human Reliability Program includes a detailed, federally mandated psychological evaluation process for individuals who work in and/or guard special and nuclear material (Reynolds *et al.*, 2015). The program relies upon a medical assessment and monitoring process to identify and mitigate safety and security risks. A component of the medical assessment involves identifying psychological vulnerabilities that may affect safety related to access to Special Nuclear Material. For instance, the Predictors of Emergent Risk and Integrity Lapses study conducted at the Y-12 National Security Complex described an effort to assess for mental disorders, personality disorders, behavioral problems, and substance abuse and misuse, as well as concerns related to suicidality, homicidality, and/or physical harm (Reynolds *et al.*, 2015). Y-12 applicant evaluations are comprehensive and include, but are not limited to, a semi-structured interview, mental status exam, cognitive testing, self-reported psychopathology testing, and a job-task analysis. Employees also undergo ongoing monitoring and assessment, including annual psychological examinations.

In contrast to the Federal Government, many municipal and state law enforcement and public safety organizations do assess all applicants. Along with a clinical interview, these organizations typically use a combination of measures such as the California Personality Inventory, Minnesota Multiphasic Personality Inventory (MMPI-2) or MMPI-2-RF, Inwald Personality Inventory (IPI), Sixteen Personality Factor Questionnaire, and/or the Personality Characteristics Inventory to identify psychopathology and assess personality (Cochrane, Tett, & Vandecreek, 2003; Sellbom, Fischler, & Ben-Porath, 2007; Stickle, 2016). Of these assessments, experts consider the MMPI-2 and MMPI-2-RF to be among the most robust tests to assess personality traits and psychopathology (Sellbom *et al.*, 2007; Sellbom, 2019).

Used commonly in the public safety domain, the MMPI-2-RF is used to screen out candidates suspected of mental health or other clinical considerations that could affect their performance (Corey & Ben-Porath, 2018). For example, all Federal Aviation Administration air traffic control specialist candidates complete the MMPI-2 as part of a

Tier 1 screening program. Applicants who meet certain thresholds then proceed to Tier 2, which may include a re-administration of the MMPI-2 (with a warning to be honest if initial results indicated defensive responding), and a clinical interview (Williams & King, 2010). The assigned psychologist then recommends whether the candidate is medically qualified for the position.

The public safety sector also leverages the IPI, an instrument designed to predict problematic behavior in law enforcement officer candidates. The IPI is a structured measure of various personality characteristics and behavioral patterns specific to psychological fitness (Super, 2006). Again, the primary goal is to screen out individuals with psychopathology that may be of particular concern.

BEST PRACTICES & LESSONS LEARNED

In addition to the individual predispositions of interest and the type of psychological assessments currently in use, several best practices and lessons learned emerged from the literature review and the SME interviews. The following sections summarize the three most common considerations.

Psychological Assessments are Resource-Intensive

It is important to note that most validated psychological assessments, especially those that assess clinical domains, are time-intensive and require substantial expertise to administer effectively. Coupled with the cost of buying test protocols and administrations, this process is expensive. Moreover, although individual personality measures have demonstrated utility in both predicting job performance and employee selection, researchers recommend an array of measures and multiple sources of information to provide a comprehensive assessment of each applicant. For example, some researchers have emphasized that a psychological assessment should consist of no fewer than two psychological tests designed to measure both normal and abnormal personality functioning (Corey & Ben-Porath, 2018). Assessment processes also should include combinations of specific job-relevant items or scales related to personality (Arrigo & Claussen, 2003).

Applicants Often Misrepresent Themselves

Many of the screening approaches detailed above include clinical assessments specifically designed for use in high-stakes contexts, or those situations in which the results of the evaluation process could have a substantial effect on the test taker's life. Such contexts can significantly affect the validity of a test taker's responses. Although any psychological evaluation carries the risk of potential deception, the risk of invalid responding increases notably in high-stakes contexts, such as in pre-employment selection (Levashina, 2018).

Misrepresentation in testing can be intentional or unintentional. Research suggests, however, that 24 to 50 percent of job applicants engage in intentional response distortion in an effort to appear as good candidates (Levashina, 2018). This distortion can lead to invalid and unreliable scores on different measures, particularly those focused on

dysfunction (Detrick & Chibnall, 2014). For example, applicants may be motivated to mask psychological problems or exaggerate virtues and personality characteristics they believe reflect an ideal applicant (Detrick & Chibnall, 2014; Levashina, 2018). This may be particularly true in the case of malicious infiltrators who are especially motivated to minimize traits or mental health symptoms or diagnoses they believe could prevent them from obtaining a job with a target organization.

Alternative approaches, such as the Shedler-Westen Assessment Procedure/Dispositional Indicators of Risk Exposure (SWAP/DIRE), rely on clinician reports rather than applicants' self-reports (Lang & Shechter, 2011). Moreover, the SWAP/DIRE also is the only scale specifically focused on security. However, the SWAP/DIRE takes substantial time and expertise, as it requires a clinician to administer an interview followed by scoring. Altogether, the interview and scoring procedure take three to three-and-a-half hours per person. Although results of a field test with the DOE suggested clinicians thought the procedure added value, the time and labor required was a substantial concern (Lang & Shechter, 2011; Shechter & Lang, 2011). Nonetheless, it remains an alternative to self-report to address the issue of applicant deception.

Hiring Policies Have Practical Concerns

In addition to the theoretical considerations relevant to identifying and measuring pertinent individual predispositions, an important factor to consider in discussing a screening program is the effect it may have on the applicant and employee population. For instance, there are substantial concerns related to applicant and employee morale (Noonan, 2018; Rona *et al.*, 2006; Shaw *et al.*, 2009). That is, subjecting people to a higher level of scrutiny can lead to concerns regarding privacy and to worries of profiling or targeting.

In addition, high-stakes testing introduces the risk that applicants will seek coaching to maximize their chance of selection. For example, some open source websites provide information to test takers about how to falsify test results. Widespread use of such sites is a distinct possibility if DoD implements mandatory psychological screening on a large scale.

Furthermore, the associations between individual predispositions and insider attack behavior are likely to be small on average, although they are comparable in size to well-accepted associations such as the link between intelligence and occupational attainment (Roberts, Kuncel, Shiner, Caspi, & Goldberg, 2007). Recent research suggests that the associations between individual predispositions and consequential life outcomes are, in general, reliable and replicable (Soto, 2019); however, the overall size of the effects suggests that there are many people for whom their level of a trait may not be associated with later insider attacks. This is equivalent to the consideration that most people who possess a trait are unlikely to commit an insider attack. However, detecting even a single attack before it occurs is obviously a significant outcome. Thus, although the cost of screening applicants is high, the cost will be higher if unscreened personnel go on to commit an insider attack (Cochrane, Tett, & Vandecreek, 2003; King, Schroder, Manning,

Retzlaff, & Williams, 2008). In short, there is a necessary balance between the cost of implementing psychological screening and its potential efficacy.

Finally, with mental health symptoms and diagnoses specifically, there also is a potential risk of increased stigma associated with screening (Rona *et al.*, 2006; Shedler & Lang, 2005). This increased stigma may lead individuals to avoid treatment for mental health symptoms or diagnoses, which could further exacerbate the potential for adverse effects on a person's well-being and work performance.

CONCLUSION

Overall, the body of empirical knowledge in the area of insider threat is unequivocal: individual predispositions are relevant to the risk of insider attacks. There are, however, a number of considerations with regard to expanding DoD's psychological screening program to include most, if not all applicants. What follows is an overview of this project's major findings, along with corresponding recommendations, limitations, and suggestions for future research.

FINDINGS & RECOMMENDATIONS

Finding #1: Although there is solid evidence that individual predispositions are related to the risk of insider attacks, additional research is required prior to large-scale implementation of psychological screening in DoD.

Relevant case studies have revealed that there is no single accepted profile of an insider attacker (Noonan, 2018; Randazzo, Keeney, Kowalski, Cappelli, & Moore, 2005). Given this variability, it is hard to determine *which* individual predispositions among those identified as empirically relevant matter most. Addressing this question would require testing associations among various factors thought to be relevant in a systematic, simultaneous, and statistical manner. Because insider attacks are rare and occur outside of a laboratory setting, this is a significant challenge and limitation to existing and future research.

In addition, some individual predispositions (*e.g.*, introversion, narcissism) that are empirically relevant to insider threat are statistically common and, therefore, would result in many false positives if used for prediction. Although this limitation is not unique to this domain, it nonetheless affects the potential utility of assessing predispositions among applicants as a way to prevent future insider attacks.

Also, while traits such as those included in the Dark Triad and the Big Five are empirically relevant to the risk of insider attacks, it is unclear at what *levels* these traits may confer an increased risk to DoD. For example, there is evidence that some aspects of The Big Five, such as low levels of agreeableness, extraversion, or conscientiousness, or high levels of neuroticism, are relevant to insider attacks, but substantial work remains to determine at what level and/or combination they become a concern (Egan & Lewis, 2011; Salgado, 2002; Shaw *et al.*, 1998).[4]

Finally, tests for individual predispositions are not without controversy, and any assessment should be just one part of a larger, comprehensive screening program designed for a particular position or organization (Shaw *et al.*, 2009). As mentioned, this comes with significant resource challenges.

[4] Note that there is promising work showing predictive validity for sub-clinical levels of some individual predispositions in the area of law enforcement screening that might be used to help address this concern (*e.g.*, Tarescavage, Brewster, Corey, & Ben-Porath, 2015).

Recommendation #1a: DoD should explore the links among personality dysfunction, psychopathology assessments, and pre-attack behaviors, such as CWBs, which occur at a greater frequency than insider attacks. Such a study could help to identify the incremental utility of using well-established tools in multiple domains (*e.g.*, MMPI, Dark Triad, Big Five) and also identify the level at which different personality traits may relate to problematic behaviors, including concerns associated with insider attacks.

Recommendation #1b: DoD should review the classified literature on individual predispositions and insider attacks. SME discussions suggested that there are approaches within the classified domain that may provide useful information for DoD's Counter Insider Threat Program, but further research is necessary to understand those processes and their value.

Finding #2: All of the SMEs consulted for this effort suggested DoD should expand psychological screening to include more, *but not all*, applicants.

SMEs emphasized that insider threat is a human problem, and that identifying risk requires a deep understanding of the individual. One SME, in particular, emphasized that clinical interviews identify a large amount of unique information not found elsewhere during an individual's background investigation.

Although the challenges associated with screening large numbers of individuals are not the only considerations in developing screening programs, the practical implications cannot and should not be ignored. In fact, there is a necessary balance between the cost of implementing psychological screening and its potential efficacy.

Recommendation #2a: Screening every applicant is not feasible. Instead, screening should focus first on individuals who present the highest risk due to job position (*e.g.*, seniority or access to sensitive information), and DoD should further triage based on the results of an assessment process to identify even smaller groups of individuals for more extensive psychological evaluation.

Recommendation #2b: Psychological assessments only at the time of application are insufficient, as individual risk changes over time. Organizations across DoD should use psychological screening to assess employees for cause (*e.g.*, reports from co-workers, supervisors) during the course of their careers.

Finding #3: Psychological screening must consider the likely possibility that applicants will misrepresent themselves.

There is evidence in the literature that applicants often misrepresent themselves in high-stakes contexts. One way to address concerns about deception is to use embedded validity scales, which identify when an individual's test scores are suspicious. For example, the Personality Assessment Inventory (PAI), MMPI-2, and MMPI-2-RF contain well-validated embedded validity scales (Ben-Porath & Tellegen, 2011; Butcher *et al.*, 2001; Morey,

2007). There also are stand-alone measures of social desirability and impression management. Although commonly used, these measures, such as the Paulhus Deception Scales (Paulhus, 1998) and Marlowe-Crowne Social Desirability Scale (Crowne & Marlowe, 1960), have been criticized as measuring conscientiousness and neuroticism more than response bias (Levashina, 2018). In contrast, embedded validity indicators on the PAI, MMPI-2, and MMPI-2-RF have been demonstrated to be sensitive to invalid test responding and can alert examiners to test results that do not accurately reflect an examinee's standing on the trait of interest (Burchett & Bagby, 2014).

> **Recommendation #3**: Screening programs should include tools with well-validated embedded validity scales to address concerns of applicant deception (*e.g.*, PAI, MMPI-2, MMPI-2-RF). Any screening program should include these assessments as part of a broader applicant assessment process that leverages a whole-person approach.

LIMITATIONS

As previously noted, Appendix A summarizes the case studies of previous insider attacks that identified most of the predispositions reviewed for this project. While these case studies provide rich detail regarding the nature of the actors, the events themselves, and their aftermath, they also have important limitations. For instance, case studies lack statistical robustness. That is, case studies may allow researchers to infer interactions or concepts that may be important, but they cannot provide generalizable information regarding any specific factor and its association with insider attacks. Also, they cannot provide detailed information about the strength of the association between any single predisposition and the risk of insider attack. Thus, although there is empirical evidence and support from SMEs that predispositions are important to understanding the risk of insider attacks, evidence regarding the strength of this association and its generalizability is limited. Results of this and other similar reviews should, therefore, be interpreted cautiously. Further, SMEs provided information given their knowledge and expertise, which is by nature somewhat limited. Other individuals (*i.e.*, from fields of study outside of psychology) may have different perspectives. Thus, SME opinions presented here may not represent the insider threat stakeholder community.

FUTURE RESEARCH

First, in addition to the follow-up research already recommended, it is important to design any new security initiative in such a way that its potential value may be measured. For example, if DoD were to expand psychological screening to more applicants as a way to prevent insider attacks, organizations must know the current baseline against which they will measure future success. Because insider attacks are rare, it would make more sense to measure baseline rates of pre-attack behaviors (*e.g.*, CWB), implement expanded psychological screening, and then measure rates post-implementation. This type of research is extremely rare and when it is done, organizations rarely release it publicly.

Second, three SMEs suggested follow-up research related to individuals' fit with their job, role, or position. In general, SMEs suggested that person-job misfit may lead to additional stress or concerns for the individual that may increase the risk of insider threat. The literature also includes misfit as a potential indicator, at least indirectly (Greitzer *et al.*, 2009). Unlike the characteristics summarized in this report, however, job misfit does not qualify as an individual predisposition. It is not a characteristic of the individual, but an association between that individual and his/her current role or position. However, organizations could use individual predispositions (*e.g.*, personality traits, social skills) to assess whether or not an individual would be a good fit for a particular job. For example, organizations may define individual predispositions that are important to function well for a specific position, and then assess the degree to which an applicant possesses those characteristics. Notably, this emphasis on fit allows for a somewhat more positive view of psychological screening. That is, organizations can highlight predispositions that make an individual a good fit to perform well in a particular role. However, note that screening out specific predispositions may actually screen out individuals who are well-suited to specific jobs, but simply require different styles of management (Osumi & Ohira, 2010). Research is needed to determine the utility of increasing job fit as a strategy to prevent insider attacks.

REFERENCES

Anderson, D., Moore, A. P., Stanton, J. M., Cappelli, D. M., Rich, … & Zagonel, A. (2004). Preliminary system dynamics maps of the insider cyber-threat problem. *International Conference of the Systems Dynamics Society,* 25-29.

Arrigo, B. A., & Claussen, N. (2003). Police corruption and psychological testing: A strategy for preemployment screening. *International Journal of Offender Therapy and Comparative Criminology, 47*(3), 272-290.

Ashton, M. C., & Lee, K. (2007). Empirical, theoretical, and practical advantages of the HEXACO model of personality structure. *Personality and Social Psychology Review*, *11*(2), 150–166.

Azizli, N., Atkinson, B., Baughman, H., Chin, K., Vernon, P., Harris, E., & Veselka, L. (2016). Lies and crimes: Dark triad, misconduct, and high-stakes deception. *Personality and Individual Difference, 89*, 34-39.

Band, S. R., Cappelli, D. M., Fischer, L. F., Moore, A. P., Shaw, E. D., & Trzeciak, R. F. (2006). *Comparing insider IT sabotage and espionage: A model-based analysis* (No. CMU/SEI-2006-TR-026). Carnegie Mellon University Software Engineering Institute: Pittsburgh, PA.

Ben-Porath, Y. S., & Tellegen, A. (2011). *MMPI-2-RF manual for administration, scoring, and interpretation.* Minneapolis: University of Minnesota Press.

Bergstrøm, H., Larmour, S. R., & Farrington, D. P. (2018). The usefulness of psychopathy in explaining and predicting violence: Discussing the utility of competing perspectives. *Aggression and Violent Behavior*, 84-95.

Boer, D. P., Wilson, R. J., Gauthier, C. M., & Hart, S. D. (1997). Assessing risk of sexual violence: Guidelines for clinical practice. In C. D. Webster & M. A. Jackson (Eds.), *Impulsivity: Theory, assessment and treatment* (pp. 326-342). New York, NY: Guilford

Burchett, D., & Bagby, R. M. (2014). Multimethod assessment of distortion: Integrating data from interviews, collateral records, and standardized assessment tools. In C. J. Hopwood & R. F. Bornstein (Eds), *Multimethod Clinical Assessment* (pp. 345-378). New York, NY: Guilford.

Butcher, J. N., Graham, J. R., Ben-Porath, Y. S., Tellegen, A., Dahlstrom, W. G., & Kaemmer, B. (2001). *MMPI-2: Manual for administration and scoring* (Rev. ed.). Minneapolis: University of Minnesota Press.

Cardona, R. A., & Ritchie, E. C. (2006). Psychological screening of recruits prior to accession in the U.S. military. In B. L. DeKoning, (Ed.), *Recruit Medicine. Textbooks of Military Medicine* (pp. 297–309). Borden Institute, Office of the Surgeon General. Washington, DC.

Claycomb, W. R., Huth, C. I., Flynn, L., McIntire, D. M., & Lewellen, T. B. (2012). Chronological examination of insider threat sabotage: Preliminary observations. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 3*, 4-20.

Cochrane, R. E., Tett, R. P., & Vandecreek, L. (2003). Psychological testing and the selection of police officers. *Criminal Justice and Behavior, 30*(5), 511-537.

Cohen, T. R. (2017, January/February). The morality factor. *Scientific American Mind, 28*, 32-38.

Corey, D. M., & Ben-Porath, Y. S. (2018). *Assessing police and other public safety personnel using the MMPI-2-RF: A practical guide*. University of Minnesota Press: Minneapolis, MN.

Crowne, D. P., & Marlowe, D. (1960). A new scale of social desirability independent of psychopathology. *Journal of Consulting Psychology, 24,* 349-354.

DeMatteo, D., Edens, J. F., & Hart, A. (2010). The use of measures of psychopathy in violence risk. In R. K. Otto & Douglas, K. S. (Eds.), *Handbook of violence risk assessment* (pp. 19-40). New York: Routledge.

Detrick, P., Ben-Porath, Y. S., & Sellbom, M. (2016). Associations between MMPI-2-RF (Restructured Form) and Inwald Personality Inventory (IPI) scale scores in a law enforcement preemployment screening sample. *Journal of Police and Criminal Psychology*, *31*(2), 81-95.

Detrick, P., & Chibnall, J. (2014). Underreporting on the MMPI–2–RF in a high-demand police officer selection context: An illustration. *Psychological Assessment*, *26*(3), 1044-1049.

Dickerhoof, R. M., Baweja, J. A., Osborn, M. M., & Smith, C. M. (2018). *A personnel security training program for clinicians: Phase I* (TR 18-13). Defense Personnel and Security Research Center: Seaside, CA.

DoD Manual 5210.42. *Nuclear weapons Personnel Reliability Program (Incorporating Change 1, Effective June 27, 2016*).

Draft DoD Directive 5205.16. *Countering the insider threat in the Department of Defense*.

Egan, V., & Lewis, M. (2011). Neuroticism and agreeableness differentiate emotional and narcissistic expressions of aggression. *Personality and Individual Differences, 50*, 845-850.

Fischer, L. J. (2003). *Characterizing information systems insider offenders*. Presented at the Conference of the International Military Testing Association, Pensacola, FL.

Garb, H. N. (2005). Clinical judgment and decision making. *Annual Review of Clinical Psychology*, *1*, 67-89.

Garb, H. N., Wood, J. M., & Baker, M. (2018). The Lackland Behavioral Questionnaire: The use of biographical data and statistical prediction rules for public safety screening. *Psychological Assessment*, *30*(8), 1039-1048.

Godes, O., & Lang, E. L. (2009). *Identifying personality disorders that are security risks: Phase I results* (TR 09-01). Monterey, CA: Defense Personnel Security Research Center. (For Official Use Only).

Greitzer, F. L., Kangas, L. J., Noonan, C. F., Dalton, A. C., & Hohimer, R. E. (2012, January). Identifying at-risk employees: Modeling psychosocial precursors of potential insider threats. In *System Science (HICSS), 2012 45th Hawaii International Conference on System Sciences* (pp. 2392-2401). Institute of Electrical and Electronics Engineers.

Greitzer, F. L., Paulson, P., Kangas, L., Franklin, L. R., Edgar, T. W., & Frincke, D. A. (2009). Predictive modelling for insider threat mitigation. *Pacific Northwest National Laboratory, Richland, WA, Tech. Rep. PNNL Technical Report PNNL-65204*.

Greitzer, F. L., Strozer, J., Cohen, S., Bergey, J., Cowley, J., Moore, A., & Mundie, D. (2014, January). Unintentional insider threat: Contributing factors, observables, and mitigation strategies. In *2014 47th Hawaii International Conference on System Sciences* (pp. 2025-2034). Institute of Electrical and Electronics Engineers.

Hadlington, L. (2018). The "human factor" in cybersecurity: Exploring the accidental insider. In *Psychological and Behavioral Examinations in Cyber Security* (pp. 46-63). IGI Global.

Hare, R. D. (2003). *The Psychopathy Checklist – Revised* (2nd Ed.). Toronto: Multi-Health Systems.

Hare, R. D., & Neumann, C. S. (2005). Structural models of psychopathy. *Current Psychiatry Reports, 7,* 57–64.

Harris, M. A. (2012). Managing corporate computer crime and the insider threat: The role of cognitive distortion theory. *Journal of Information System Security, 8*(2), 19-41.

Jakobwitz, S., & Egan, V. (2006). The dark triad and normal personality traits. *Personality and Individual Differences*, *40*, 331-339.

Jaros, S.L. (2017). A strategic plan for leveraging the social and behavioral sciences to counter the insider threat (MR 17-07). Seaside, CA: Defense Personnel and Security Research Center. (For Official Use Only.)

John, O. P., & Srivastava, S. (1999). The big five trait taxonomy: History, measurement, and theoretical perspectives. In L. A. Pervin & O. P. John (Eds.), *Handbook of personality: Theory and research* (pp. 102-138). New York: Guilford Press.

Jones, E., Hyams, K. C., & Wessely, S. (2003). Screening for vulnerability to psychological disorders in the military: An historical survey. *Journal of Medical Screening, 10*(1), 40-46.

Kandias, M., Galbogini, K., Mitrou, L., & Gritzalis, D. (2013). Insiders trapped in the mirror reveal themselves in social media. In J. Lopez, X. Huang, & R. Sandhu (Eds.), *Network and system security. NSS 2013. Lecture notes in computer science* (Vol. 7873, pp. 220-235). Springer: Verlag Berlin Heidelberg.

Keeney, M., Kowalski, E., Cappelli, D., Moore, A., Shimeall, T., & Rogers, S. (2005). *Insider threat study: Computer system sabotage in critical infrastructure sectors*. Carnegie Mellon University Software Engineering Institute: Pittsburgh, PA.

Kiefer, C., & Benit, N. (2016). What is applicant faking behavior? A review on the current state of theory and modeling techniques. *Journal of European Psychology Students, 7*(1), 9-19.

Kowalski, E., Conway, T., Keverline, S., Williams, M., Cappelli, D., Willke, B., & Moore, A.P. (2008). *Illicit cyber activity in the government sector*. Carnegie Mellon University Software Engineering Institute: Pittsburgh PA.

Laajaj, R., Macours, K., Hernandez, D. A. P., Arias, O., Gosling, S. D., Potter, J., Robio-Codina, M., & Vakis, R. (2019). Challenges to capture the big five personality traits in non-WEIRD populations. *Science Advances*, *5*(7).

Lang, E.L. and Shechter, O.G. (2011, May). *Improved assessment of personality disorders that are security risks*. Presentation at the meeting of the International Applied Military Psychology Symposium, Vienna, Austria.

Levashina, J. (2018). Evaluating deceptive impression management in personnel selection and job performance. In R. Rogers & S. D. Bender (Eds.), *Clinical assessment of malingering and deception* (4th ed.) (pp. 530-551). New York: Guilford.

Liang, N., Biros, D. P., & Luse, A. (2016). An empirical validation of malicious insider characteristics. *Journal of Management Information Systems, 33*(2), 361-392.

Maasberg, M., Warren, J., & Beebe, N. L. (2015). *The dark side of the insider: Detecting insider threat through examination of Dark Triad personality traits*. Paper presented at the 48th Hawaii International Conference on System Sciences.

McCrae, R., & Costa, P. (1987). Validation of the Five Factor Model of personality across instruments and observers. *Journal of Personality and Social Psychology*, *52*(1), 81-90.

Moore, A. P., Cappelli, D. M., Caron, T. C., Shaw, E., Spooner, D., & Trzeciak, R. F. (2011). *A preliminary model of insider theft of intellectual property* (No. MU/SEI-2011-TN-013). Carnegie-Mellon University Software Engineering Institute, Pittsburgh, PA.

Morey, L. C. (2007). *Personality Assessment Inventory professional manual*, 2nd ed. Odessa, FL: Psychological Assessment Resources.

Mount, M., Ilies, R., & Johnson, E. (2006) Relationship of personality traits and counterproductive work behaviors: The mediating effects of job satisfaction. *Personnel Psychology, 59*, 591-622.

Noonan, C. F. (2018). *Spy the lie*. Richland, WA: Pacific Northwest National Laboratory.

Nurse, J. R. C., Legg, P. A., Buckley, O., Agrafiotis, I., Wright, G., Whitty, M., … & Creese, S. (2014). *A critical reflection on the threat from human insiders – its nature, industry perceptions, and detection approaches*. Paper presented at the International Conference on Human Aspects of Information Security, Privacy, and Trust, Heraklion, Crete, Greece.

Osumi, T., & Ohira, H. (2010). The positive side of psychopathy: Emotional detachment in psychopathy and rational decision-making in the ultimatum game. *Personality and Individual Differences*, *49*, 451-456.

Paulhus, D. L. (1998). *Paulhus Deception Scales (PDS): The Balanced Inventory of Desirable Responding-7: User's manual.* North Tanawanda, NY: Multi-Health Systems.

Paulhus, D., & Williams, K. (2002). The Dark Triad of personality: Narcissism, Machiavellianism, and psychopathy. *Journal of Research in Personality*, *36*, 556-563.

Reynolds, R. V., Rahmanian, N. B., Ritter, K., Carmody, P., Ardiaz, M., Lang, E. L., … & Stuart, G. L. (2015). *Predictors of Emergent Risk and Integrity Lapses (PERIL)* (No. OHS 2014-0011). Consolidated Nuclear Security, LLC: Oak Ridge, TN.

Randazzo, M. R., Keeney, M. M., Kowalski, E. F., Cappelli, D. M., & Moore, A. P. (2005). *Insider threat study: Illicit cyber activity in the banking and finance sector.* Carnegie Mellon University Software Engineering Institute: Pittsburgh PA.

Roberts, B., Kuncel, N., Shiner, R., Caspi, A., & Goldberg, L. (2007). The power of personality: The comparative validity of personality traits, socioeconomic status, and cognitive ability for predicting important life outcomes. *Perspectives on Psychological Science*, *2*, 313-345.

Rona, R. J., Hooper, R., Jones, M., Hull, L., Browne, T., Horn, O., … & Wessely, S. (2006). Mental health screening in armed forces before the Iraq war and prevention of subsequent psychological morbidity: Follow-up study. *British Medical Journal, 333*, 1-5. doi: 10.1136/bmj.38985.610949.55

Salgado, J. F. (2002). The Big Five personality dimensions and counterproductive behaviors. *International Journal of Selection and Assessment, 10,* 117-125.

Sellbom, M. (2019). The MMPI-2-RF Restructured Form (MMPI-2-RF): Assessment of personality and psychopathology in the twenty-first century. *Annual Review of Clinical Psychology, 15*, 149-177.

Sellbom, M., Fischler, G. L., & Ben-Porath, Y. S. (2007). Identifying MMPI-2 predictors of police officer integrity and misconduct. *Criminal Justice and Behavior*, 34, 985–1004. doi: 10.1177/0093854807301224

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

Shaw, E. D., Fischer, L. F., & Rose, A. E. (2009). *Insider risk evaluation and audit* (TR 09-02). Defense Personnel and Security Research Center: Monterey, CA.

Shaw, E., Ruby, K., & Post, J. (1998). The insider threat to information systems: The psychology of the dangerous insider. *Security Awareness Bulletin*, *2*(98), 1-10.

Shaw, E., & Sellers, L. (2015). Application of the critical-path method to evaluate insider risks. *Studies in Intelligence*, *59*(2), 41-48.

Shaw, E. D., & Stock, H. V. (2011). *Behavioral risk indicators of malicious insider theft of intellectual property: Misreading the writing on the wall.* Symantec White Paper.

Shechter, O. G., & Lang, E. L. (2011). *Identifying personality disorders that are security risks: Field test results.* Defense Personnel Security Research Center: Monterey, CA.

Shedler, J., & Lang, E. L. (2015). *A relevant risk approach to mental health inquiries in Question 21 of the Questionnaire for National Security Positions (SF-86).* Defense Personnel and Security Research Center: Seaside, CA.

Skeem, J., & Cooke, D. (2010). Is criminal behavior a central component of psychopathy? Conceptual directions for resolving the debate. *Psychological Assessment*, *22*(2), 433-445.

Stickle, B. (2016). A national examination of the effect of education, training and pre-employment screening on law enforcement use of force. *Justice Policy Journal, 13*(1), 1-15.

Super, J. T. (2006). A survey of pre-employment psychological evaluation tests and procedures. *Journal of Police and Criminal Psychology, 21*(2), 83-87.

Tarescavage, A. M., Brewster, J., Corey, D. M., & Ben-Porath, Y. S. (2015). Use of prehire Minnesota Multiphasic Personality Inventory-2–Restructured Form (MMPI-2-RF) police candidate scores to predict supervisor ratings of posthire performance. *Assessment, 22*(4), 411-428.

Wilder, U. M. (2017). The psychology of espionage. *Studies in Intelligence, 61,* 19 – 36.

Williams, C. A., & King, R. E. (2010). *The effects of testing circumstance and education level on MMPI-2 correction scale scores.* Federal Aviation Administration Civil Aeromedical Institute: Oklahoma City, OK.

Wright, K. M., Huffman, A. H., Adler, A. B., & Castro, C. A. (2002). Psychological screening program overview. *Military Medicine, 167*(10), 853-861.

Wright, K. M., Thomas, J. K., Adler, A. B., Ness, J. W., Hoge, C. W., & Castro, C. A. (2005). Psychological screening procedures for deploying U.S. Forces. *Military Medicine, 170*(7), 555-562.

APPENDIX A: CASE STUDIES OF INSIDER THREAT

Case studies have advanced the insider threat discipline, as they describe in rich detail both the individual predispositions and situational factors that precipitated specific insider attacks. As shown in Table 1, many of these case studies emerged from the National Insider Threat Center, CERT Division, Software Engineering Institute (CERT) with much of the early research completed during a collaboration with the United States Secret Service (USSS) in the late 1990s and early 2000s (*e.g.*, Band *et al.*, 2006; Keeney *et al.*, 2005; Kowalski *et al.*, 2008; Moore *et al.*, 2011; Randazzo, Keeney, Kowalski, Cappelli, & Moore, 2005).

Although the studies varied in method, researchers most commonly applied a system dynamics approach—a method for modeling complex systems over time (Band *et al.*, 2006). Using this approach, researchers studied previous instances of insider threat, focusing either on particular types of attacks (*e.g.,* sabotage, espionage, or theft of intellectual property) or on insiders in particular sectors (*e.g.,* critical infrastructure, banking, or finance; Band *et al.*, 2006; Kowalski *et al.*, 2008; Moore *et al.*, 2011; Randazzo *et al.*, 2005). These studies resulted in a series of detailed models that demonstrated the interaction among aspects of the individual, the organization, and events, and provided insight into the patterns revealed in these different types of insider threat.

Other studies used the comparative case method, reviewing the similarities and differences among different instances of insider threat (*e.g.*, Shaw & Fischer, 2005). In doing so, researchers divided perpetrators into types (*e.g.*, the Machiavellian Leader, the Entitled Disgruntled Thief) to provide a greater understanding of the nature of the events, insiders, and organizations involved (Shaw & Stock, 2011).

For each study, Table 1 presents the case selection criteria, the number of insiders and incidents, the years the incidents occurred, the materials used during the study (*e.g.*, open source, investigative materials, interviews), and a brief summary. Psychological data in these studies (*i.e.*, self-report, interviews) are rare; however, some of the studies included interviews with the perpetrators. While it is tempting to conclude that these studies are more valid because insiders themselves provided information regarding their psychological characteristics and motivations, they may provide biased information (*e.g.*, broaching a narrative that they were treated unfairly; Shaw & Fischer, 2005).

Table 1
Case Studies of Insider Threat

Reference	Sample Description	Sample Size	Incident Year(s)	Materials	Summary
Anderson *et al.*, 2004	Selected well-known cases of insiders with organizations that had a very trusting environment for certain classes of employees, who then successively tested and/or lessened the security controls, helping to avoid detection and create maximum damage.	*n* = 6	No years provided	Cases reviewed were well-documented in the public domain; paper does not suggest that any material other than publicly available information (*e.g.*, newspaper articles, court records) was used.	Presents a system dynamics approach to insider threat on the basis of six well-known cases of insider threat. The generalizations and models proposed are the result of a workshop, and are preliminary hypotheses regarding the nature of insider threat.
Band *et al.*, 2006	Selected information technology (IT) sabotage cases from the Insider Threat Study based on information available to meet the needs of the system dynamics approach; PERSEREC selected espionage cases based on same criteria.	*n* = 30 IT sabotage cases; *n* = 9 espionage cases	No years for sabotage cases; espionage cases 1986-2004	Researchers reviewed case documentation and interviews, including peer and supervisor reports. In some cases, insiders were available for interview (exact number of interviews not specified).	Part of the Insider Threat Study collaboration between CERT and USSS. Goal was to compare the similarities and differences between sabotage and espionage cases to determine if they could be modeled using the same framework. Applied system dynamics to create models of the two types of insider threat.
Claycomb, Huth, Flynn, McIntire, & Lewellen, 2012	Selected cases in the U.S. that were part of critical infrastructure and based on a score generated on the basis of data availability and the number of events, choosing the top-scoring cases.	*n* = 15	2008 - 2012	Data were from a database of insider activity, and included public court documents, law enforcement investigations, and interviews with insiders.	Presents the results of case studies with the goal of identifying key points of interest in the chronology of events during an insider attack, including attacker disgruntlement, preparations, initiation, attack end, and attack detection, followed by insider consequences.
Fischer, 2003	Selected Information Systems insiders (people who held a position of trust and were given access to defense information systems) as part of the Insider Events Database at PERSEREC	*n* > 80 (no exact sample size)	No years provided; example cases occurred in mid-1990s	Information was taken from the *Insider Events Database* developed at PERSEREC, but the materials involved are not described.	Presents generalizations and findings from the case studies of information systems insiders, and provides a sample case study for each finding.

Reference	Sample Description	Sample Size	Incident Year(s)	Materials	Summary
Keeney *et al.*, 2005	Selected cases in which the insider's primary goal was sabotage of the organization or direct harm of an individual through misuse of access or exceeding access; all cases occurred in the U.S. and were part of critical infrastructure.	*n* = 49	1996 - 2002	Researchers reviewed primary source material including investigative records, court records, and others, as well as secondary materials such as news articles. Researchers conducted interviews with case investigators and organization representatives. One insider was interviewed.	Presents results of the Insider Threat Study focused specifically on sabotage. Provides information on characteristics of insiders, their organizations, and the consequences of the attack. The report also describes generalizations from the attacks, such as motive, pre-attack behavior and planning, and attack detection.
Kowalski *et al.*, 2008	Selected insider cases in the government sector, defined as Federal, State, and local government agencies, and private agencies contracted to serve as arms of the government or other private franchised organizations that provide services on behalf of the government.	*n* = 36 insiders; *n* = 38 incidents	1996 - 2002	Researchers reviewed law enforcement reports, court records, mental health records, arrest records, third-party accounts of the insider's history and behavior, and news articles. When possible, researchers interviewed case investigators, organization representatives, prosecutors, and insiders (number not specified).	Part of the Insider Threat Study collaboration between CERT and USSS. Presents results of case studies of incidents in the government sector, focusing on the characteristics of the insiders, the incidents, the detection of the incidents, and the consequences.
Moore *et al.*, 2011	Presented case studies of theft of intellectual property for crimes in the U.S., studied through public records. Theft of intellectual property is defined as crimes in which access was misused or exceeded to steal confidential or proprietary information. Cases were selected on the basis of available information.	*n* = 48	2002 - ?	Researchers used public reporting and primary source materials such as court records and secondary sources such as media reports.	Study from CERT using system dynamics and comparative case method to define two types of cases within the category of theft of intellectual property: the entitled independent and the ambitious leader. Results described the nature of the insider (including personal characteristics) as well as the incidents themselves, their detection, and the consequences for the organization.

Reference	Sample Description	Sample Size	Incident Year(s)	Materials	Summary
Nurse *et al.*, 2014	Stated no specific criteria for selecting cases other than availability of information (described more in "Materials"). Additional cases were added via direct means, although no specific criteria or characteristics were described.	*n* = 80 in initial sample; *n* = 99 additional; total *N* = 149	No years provided	Researchers relied on information from CERT's database and the United Kingdom's Centre for the Protection of National Infrastructure, as well as news articles.	The goal was to present a unifying framework for insider threat using the case studies included. Following initial development, the framework was applied to the additional cases for confirmation. The framework outlines characteristics of the actor, attack, and organization, as well as the catalyst that incited the attack.
Randazzo *et al.*, 2005	Identified insiders through public reporting (*e.g.*, LexisNexis, Google) or computer fraud cases investigated by USSS; focused specifically on cases in the banking and finance sector (*e.g.*, credit unions, banks, investment firms)	*n* = 26 insiders; *n* = 23 incidents	1993 - 2002	Researchers reviewed investigative reports, court records, news articles, and other material, and conducted interviews with case investigators and organization representatives (number not specified). Two insiders were interviewed.	Part of the Insider Threat Study collaboration between CERT and USSS. Conducted case studies to understand characteristics of the incident, the insider, the attack and subsequent harm, and the law enforcement and organizational response.
Shaw & Fischer, 2005	Selected cases with criminal conviction, confession, or other means of verification, with preference given to individuals who were part of the U.S. critical national infrastructure of Defense/Government contractors. Location was limited to the DC/NY corridor. Cases were selected that had accessible private or public materials, such as investigators, prosecutors, or peers.	*n* = 10	1995 - 2002	Researchers used news media reports, law enforcement records, court documents, and interviews with prosecutors, coworkers, investigators, and (in three of 10 cases) the subjects themselves.	Presents generalizations from 10 case studies from PERSEREC using the comparative case method. Describes characteristics of the attackers as well as proposed subtypes of perpetrators.

Note. It is unclear how these different case studies overlap. Although they were presented in different papers, it is likely that some or even many of the cases were the same. Furthermore, Table 1 is not an exhaustive list but instead, represents some of the better-known and larger studies.

APPENDIX B: INDIVIDUAL PREDISPOSITIONS AND INSIDER THREAT

Table 2 presents specific citations for the predispositions researchers have found to be associated with insider attacks. Each row displays a broad predisposition, followed by a more specific predisposition, and finally, the citation(s) in which the predisposition was identified.

Table 2
Individual Predispositions and Insider Threat

Broad Predisposition	Specific Predisposition	Citation
Machiavellianism	None specified	Nurse *et al.*, 2014; Shaw & Stock, 2011
Narcissism [b]	None specified	Kandias *et al.*, 2013; Nurse *et al.*, 2014; Shaw & Sellers, 2015
Narcissism	Sensitivity to Criticism	Band *et al.*, 2006
Narcissism	Need for Attention	Band *et al.*, 2006
Narcissism	Sense of Entitlement[b]	Band *et al.*, 2006; Moore *et al.*, 2011; Shaw *et al.*, 1998; Shaw & Stock, 2011; Wilder, 2017
Narcissism	Grandiosity	Band *et al.*, 2006; Wilder, 2017[a]
Narcissism	Excessive Ego	Band *et al.*, 2006; Wilder, 2017[a]
Narcissism	Malignant Narcissism	Godes & Lang, 2009[a]
Psychopathy[b]	None specified	Godes & Lang, 2009[a]; Nurse *et al.*, 2014; Shaw & Sellers, 2015
Psychopathy	Exploitativeness	Wilder, 2017[a]
Psychopathy	Empathy Problems	Band *et al.*, 2006; Shaw & Stock, 2011; Wilder, 2017[a]
Psychopathy	Thrill-seeking	Wilder, 2017[a]
Psychopathy	Impulsivity[b]	Band *et al.*, 2006
Agreeableness (Low)	Agreeableness (Low)	Egan & Lewis, 2011[a]; Moore *et al.*, 2011
Conscientiousness (Low)	Conscientiousness (Low)	Moore *et al.*, 2011
Extraversion (Low)	Extraversion (Low)	Shaw *et al.*, 1998

Broad Predisposition	Specific Predisposition	Citation
Neuroticism (High)	Neuroticism (High)	Egan & Lewis, 2011[a]
Honesty-Humility[c] (Low)	Honesty-Humility (Low)	Cohen, 2017[a]
Emotional Issues	Chronic Frustration/Feelings of Being Unappreciated	Band *et al.*, 2006; Greitzer *et al.*, 2012
Emotional Issues	Inappropriate Anger/Propensity to Anger	Band *et al.*, 2006; Greitzer *et al.*, 2012; Shaw *et al.*, 1998
Emotional Issues	Disgruntlement[b]	Greitzer *et al.*, 2012; Liang *et al.*, 2016; Nurse *et al.*, 2014; Shaw & Fischer, 2005; Shaw *et al.*, 1998
Emotional Issues	Chronic Grudges[b]	Band *et al.*, 2006; Greitzer *et al.*, 2012
Social Deficits	Lack of social skills	Shaw *et al.*, 1998; Shaw & Stock, 2011
Social Deficits	Chronic Interpersonal Problems[b]	Band *et al.*, 2006
Social Deficits	Social Isolation	Shaw *et al.*, 1998
Mental Health Symptom or Diagnosis	Anxiety	Band *et al.*, 2006
Mental Health Symptom or Diagnosis	Depression	Band *et al.*, 2006
Mental Health Symptom or Diagnosis	Alcohol Problems[b]	Band *et al.*, 2006; Nurse *et al.*, 2014; Shaw & Sellers, 2015
Mental Health Symptom or Diagnosis	Drug Problems[b]	Band *et al.*, 2006; Nurse *et al.*, 2014
Mental Health Symptom or Diagnosis	Antisocial Personality Disorder	Liang *et al.*, 2016
Mental Health Symptom or Diagnosis	Disruptive Mood Dysregulation Disorder	Liang *et al.*, 2016
Mental Health Symptom or Diagnosis	Panic Attacks/Panic Disorder	Band *et al.*, 2006
Mental Health Symptom or Diagnosis	Avoidant Personality	Shaw & Sellers, 2015; Liang *et al.*, 2016

Broad Predisposition	Specific Predisposition	Citation
Mental Health Symptom or Diagnosis	Psychosis	Shaw & Sellers, 2015; Shedler & Lang, 2015[a]

[a] These are not case studies of insider threat directly, but are studies of related areas (*e.g.*, personnel security, aggression, CWB).
[b] These traits were identified by SMEs in addition to being discussed in the literature.
[c] Honesty-Humility is not included in the Big Five, but researchers have proposed it as an addition to the Big Five that is important in more collectivist (*e.g.*, East Asian) cultures, changing the Big Five to Humility-Honesty, Emotionality (*i.e.*, Neuroticism), Extraversion, Agreeableness, and Openness to Experience (HEXACO; Ashton & Lee, 2007).