PERSEREC

OPA-2018-082
PERSEREC-TR-18-16

October 2018

A Strategic Plan to Leverage the Social & Behavioral Sciences to Counter the Insider Threat

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

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

OPA-2018-082 **PERSEREC-TR-18-16** **October 2018**

A Strategic Plan to Leverage the Social & Behavioral Sciences to Counter the Insider Threat

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**

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

1. REPORT DATE:	2. REPORT TYPE: Technical Report	3. DATES COVERED:
4. TITLE: A Strategic Plan to Leverage the Social & Behavioral Sciences to Counter the Insider Threat	5a. CONTRACT NUMBER:	
	5b. GRANT NUMBER:	
	5c. PROGRAM ELEMENT NUMBER:	
6. AUTHOR(S): 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-TR-18-16, OPA-2018-082	
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 insider threat is, at its core, a human problem that results from a complex interaction among individual and environmental factors. The social and behavioral sciences (SBS) are well-suited to address this complicated and persistent human problem. In 2016, the Office of the Under Secretary of Defense for Intelligence partnered with the Defense Personnel and Security Research Center to design a comprehensive research plan and strategy to integrate the SBS into the DoD counter-insider threat mission space. Developed in collaboration with subject matter experts (SME) and approved by the DoD Insider Threat Program Director, this strategic plan has three goals: 1) Align SBS with DoD's counter-insider threat mission to ensure that the enterprise is well-equipped, trained, and vigilant in protecting DoD resources, personnel, installations, and equities; 2) Present a plan to drive current and future investment in SBS research; and 3) Communicate the SBS vision to senior leadership, stakeholders, and potential partners. The SME interviews resulted in five SBS Research Campaigns that together comprise the SBS Research Plan to counter malicious insider threat behavior: Employee Reporting; Technology, Tools & Data; Individual Factors; Organizational Factors; and Program Evaluation. As part of the interviews, SMEs also explained what is required for researchers to continue forward progress and execute the SBS Research Plan. Several SMEs drew on their own experiences building successful Insider Threat Programs, especially under adverse fiscal and cultural conditions. The two most commonly mentioned SME strategies for success—Tailor the Message and Build Strategic Partnerships—provide valuable lessons for SBS researchers who want to make a meaningful contribution to insider threat detection, prevention, and mitigation efforts.

14. SUBJECT TERMS: insider threat, social sciences, behavioral sciences, research plan

15. SECURITY CLASSIFICATION OF:			16. LIMITATION OF ABSTRACT:	17. NUMBER OF PAGES: 26	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

To date, much of the focus on resolving insider threat events has been on outdated technology, lax security protocols, and information siloes. While these factors may enable insider threat events, they do not cause them. If they did, prevention would be straightforward. Instead, humans cause insider threat events. Trusted insiders hack secure systems, exfiltrate closely guarded secrets, and walk directly into adversaries' traps in spite of extensive vetting, training, and monitoring. Because it is a human problem, there is no simple solution.

As the Senior Official for the DoD Insider Threat Program, the Under Secretary of Defense for Intelligence is committed to a multi-layered approach to insider threat detection, mitigation, and prevention. In furtherance of this effort, the Office of the Under Secretary of Defense for Intelligence partnered with the Defense Personnel and Security Research Center to design a strategic plan to leverage the social and behavioral sciences to counter insider threats. This report is the result of that effort.

Eric L. Lang
Director, PERSEREC

ACKNOWLEDGMENTS

The author would like to thank Amy Zegart; Matthew Bunn, Harvard University; Matthew Peoria; Nick Catrantzos, Center for Homeland Defense and Security; and representatives from the following organizations whose participation made this project possible:

AbleVets LLC
Alion Science & Technology
Applied Research Laboratories, University of Texas at Austin
CACI International, Inc.
CGI Federal
Defense Advanced Research Projects Agency
Defense Contract Management Agency
Defense Finance and Accounting Service
Defense Intelligence Agency
Defense Logistics Agency
Defense Technical Information Center
Defense Technology Security Administration
Defense Threat Reduction Agency
Department of Energy
Department of Justice
Department of State
Department of Transportation
Department of the Treasury
DoD Education Activity
DoD Test Resource Management Center
Federal Bureau of Investigation
Federal Emergency Management Agency
Haystax
Missile Defense Agency
Motorola Solutions
National Geospatial-Intelligence Agency
National Guard Bureau
National Insider Threat Center, CERT Division, Software Engineering Institute
National Insider Threat Task Force
National Security Agency
NOWHERETOHIDE.ORG
Pacific Northwest National Laboratory
Performance Accountability Council
Systems Planning and Analysis, Inc.
Talon Security Solutions, LLC
United States Air Force
United States Army
United States Coast Guard
United States Marine Corps
United States Strategic Command

EXECUTIVE SUMMARY

The insider threat is, at its core, a human problem that results from a complex interaction among individual and environmental factors. The social and behavioral sciences (SBS) are well-suited to address this complicated and persistent human problem, and there are a number of SBS efforts ongoing within and outside the federal government. Unfortunately, there is little coordinated collaboration or communication between researchers and stakeholders. As a result, the government risks blind spots or duplicated efforts, while researchers miss opportunities to share their results for the benefit of a broader audience.

In 2016, the Office of the Under Secretary of Defense for Intelligence partnered with the Defense Personnel and Security Research Center (PERSEREC) to design a comprehensive research plan and strategy to integrate the SBS into the DoD counter-insider threat mission space. Developed in collaboration with subject matter experts (SME) and approved by the DoD Insider Threat Program Director, this strategic plan has three goals:

- Align SBS with DoD's counter-insider threat mission to ensure that the enterprise is well-equipped, trained, and vigilant in protecting DoD resources, personnel, installations, and equities;
- Present a plan to drive current and future investment in SBS research; and
- Communicate the SBS vision to senior leadership, stakeholders, and potential partners.

PERSEREC completed 59 interviews with 66 SMEs who represented 45 organizations: 10 private sector companies, nine Defense Agencies, nine non-DoD federal agencies, seven federally funded research and development centers (FFRDC) and university affiliated research centers (UARC), four military Services, four DoD Field Activities, one Defense Joint Activity, and one Combatant Command.

The SME interviews resulted in five SBS Research Campaigns that together comprise the SBS Research Plan to counter malicious insider threat behavior: Employee Reporting; Technology, Tools & Data; Individual Factors; Organizational Factors; and Program Evaluation. SMEs also explained what is required to build successful Insider Threat Programs, especially under adverse fiscal and cultural conditions. The two most commonly mentioned SME strategies for success—Tailor the Message and Build Strategic Partnerships—provide valuable lessons for SBS researchers who want to make a meaningful contribution to insider threat detection, prevention, and mitigation efforts.

TABLE OF CONTENTS

INTRODUCTION

The insider threat problem is neither new nor easy to address. Before Chelsea Manning and Reality Winner, there was Ana Montes. Before Nidal Hasan and Aaron Alexis, there was William Kreutzer. Regardless of whether it manifests as espionage, unauthorized disclosure, workplace violence, or some other malicious behavior, the insider threat is, at its core, a human problem that results from a complex interplay among individual, interpersonal, and organizational factors.

The social and behavioral sciences (SBS) are well-suited to address this complicated and persistent human problem, and currently, there are relevant projects ongoing across the federal government, academia, and industry. Unfortunately, there is little coordinated collaboration or communication between researchers and stakeholders. As a result, the government risks blind spots or duplicated efforts, while researchers miss opportunities to share their results for the benefit of a broader audience.

A STRATEGIC PLAN FOR THE FUTURE

Prompted by Executive Order 13587 and the corresponding *National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs* (hereinafter "Minimum Standards"), DoD issued Directive 5205.16, *The DoD Insider Threat Program*, on September 30, 2014. Under this Directive, the Under Secretary of Defense for Intelligence was designated as the Senior Official for DoD's Insider Threat Program (ITP), responsible for "policy, strategy, plans, programs, required capabilities, and resources . . . necessary to counter insider threats" (2014, p. 8).

OUSD(I) is committed to a multi-layered approach to insider threat prevention, detection, and mitigation that integrates expert operations and analysis, robust education, and cutting edge research. In furtherance of this commitment, and in recognition of the human at the center of the insider threat, the DoD ITP includes SBS as one of its strategic pillars to "ensure that the premise of understanding human behavior becomes the foundation in analytic hub operations" (DoD Counter Insider Threat Playbook, 2018). The goals for SBS at the enterprise-level are as follows:

1. Establish governance, oversight, and a network of experts;
2. Foster collaborations to ensure research is driven by stakeholders' needs;
3. Develop enterprise-level reachback capabilities to meet local needs; and
4. Develop applied knowledge capabilities within Insider Threat Program Hubs.

In 2016, OUSD(I) partnered with the Defense Personnel and Security Research Center (PERSEREC) to design a comprehensive research plan and strategy to integrate the SBS into the DoD counter-insider threat mission space. Developed in collaboration with SMEs and approved by the DoD ITP Director, this strategic plan has three goals:

1. Align SBS with DoD's counter-insider threat mission to ensure that the enterprise is well-equipped, trained, and vigilant;
2. Present a plan to drive current and future investment in SBS research; and
3. Communicate the SBS vision to senior leadership, stakeholders, and potential partners.

METHOD

Between December 2016 and January 2018, insider threat SMEs were identified from across the federal government, academia, and the private sector, and were recruited to participate in interviews about current and future SBS research to counter the insider threat. The following sections provide an overview of the recruitment, interview, and data analysis processes.

RECRUITMENT

In total, 59 interviews were completed with 66 SMEs who represented 45 organizations: 10 private sector companies, nine Defense Agencies, nine non-DoD federal agencies, seven federally funded research and development centers and university affiliated research center universities, four military Services, four DoD Field Activities, one Defense Joint Activity, and one Combatant Command.

SME recruitment occurred in four phases. First, in December 2016, the OUSD(I) ITP Office sent a tasker to the Program Managers in charge of the then-43 DoD Component ITPs (hereinafter, "DoD tasker"). The DoD tasker explained OUSD(I)'s interest in developing an SBS Strategic Plan, and invited Program Managers to "identify . . . potential research questions and topics of interest, the answers to which are meant to help with any part of your insider threat mission (e.g., policy development, strategy/program decisions, acquisition decisions, risk management)." Two SBS research questions were provided as examples, along with definitions of both social science research and behavioral research:

> Behavioral refers to what people do, as well as what drives them and why. Social, on the other hand, refers to how people interact with each other in groups, organizations, and communities.

All Program Managers who responded to the DoD tasker were contacted via email and invited to participate in an interview.

Second, in April 2017, this project was briefed to the audience in attendance at the Federal Bureau of Investigation's second annual Insider Threat Behavioral and Technical Research Working Symposium in Dallas, Texas. Audience members were encouraged to volunteer to participate in an interview, and contact information was collected from interested parties after the briefing.

Third, in December 2017, this project was advertised in an email sent to the membership of the National Insider Threat Special Interest Group, an organization for insider threat risk mitigation security professionals in and outside of government. That same month, a notice also was included in the OUSD(I) ITP Office's monthly Insider Threat newsletter.

Finally, the majority of SMEs who participated in an interview were asked to provide names of people or organizations they believed should be contacted and invited to participate in the study. If the SME suggested an agency or organization, he/she was

asked for a specific contact name and permission to use the SME's name in a recruitment email.

INTERVIEW PROCESS

Interviews were conducted in two phases. Phase I occurred between March and May 2017, and Phase II occurred between November 2017 and January 2018. Altogether, 52 interviews were conducted via telephone and seven were done in-person. Interviews lasted approximately 1 hour. All of the interviews were conducted by the same interviewer, who simultaneously wrote field notes; a second team member also took field notes for the majority of the telephonic discussions. Six of the seven in-person interviews were conducted over a 2-day period, and were audio recorded due to the compressed schedule. All field notes were compiled and sent back to SMEs for review and final approval. The six audio recordings were deleted once the field notes received final approval.

INTERVIEW PROTOCOL

Thirteen semi-structured interview protocols were designed to accommodate SMEs' diverse organizational affiliations and occupational roles. Every protocol began with general questions about the SME's role, and then branched depending on whether or not the SME was directly involved in an organization's formal ITP. The interview protocol then branched again to discuss the SME's responses to the DoD tasker, if relevant. Those who did not respond to the DoD tasker or who were outside DoD were asked to explain their general understanding of SBS research, cite any ongoing SBS efforts in their organizations, and suggest future SBS projects.

QUALITATIVE DATA ANALYSIS

Upon completion of all 59 interviews in January 2018, the field notes were reviewed by the research team to identify repeated themes and notable quotations. These themes were organized into two categories: an SBS research plan and a strategy to execute the plan. What follows are the results of that analysis.

SBS RESEARCH PLAN

The SME interviews resulted in an overview of current SBS research efforts as well as ideas for the future. They also highlighted the fundamental principles that underlie SBS insider threat research and ITP policies and procedures more broadly. What follows is a description of these principles, and then the remainder of this section is devoted to a description of five SBS Research Campaigns that DoD should prioritize for future investment. Together, these five campaigns comprise the SBS Research Plan to counter malicious insider threat behavior. Each campaign includes several supporting quotations excerpted from SME interviews, and Appendix A includes a list of specific research questions that operationalize each SBS Research Campaign.

INSIDER THREAT PRINCIPLES

> "An Insider Threat Program is not about zeroes and ones, and it is not just counterintelligence-lite. It is about people and their pathways to an incident."
>
> - *Government SME*

Spies, hackers, leakers, and other malicious insiders vary across a number of categories, including age, race, and education. As a result, demographic profiles provide little, if any, predictive power, and, therefore, are unsuitable frameworks on which to build effective ITPs. Instead, stakeholders in the insider threat community, including SBS researchers, have based their approaches to this difficult problem on four behavioral principles:

1. The risk of becoming an insider threat is not randomly distributed throughout the workforce—certain people are more likely to pose threats.
2. Insider threats occur in a social context—certain environments are more likely to facilitate insider threat behavior.
3. A person's transformation from a trusted employee to an insider threat is a process, not an event.
4. High-impact, low frequency insider threat behavior is correlated with and preceded by far more common indicators that can be observed, modeled, and, perhaps most importantly, mitigated.

Taken together, these four principles highlight the fact that much about malicious insider threat behavior is knowable. As a result, DoD stakeholders can mitigate, if not prevent, this behavior.

EMPLOYEE REPORTING

> "Everyone is the insider threat team, not just the police or security personnel. It is everyone's responsibility to keep the agency and the mission safe."
> - *Government SME*

After-action reports from the most devastating insider threat incidents reveal that in many cases, people knew something was wrong but did not report it. As one government SME explained, "Bradley Manning, Edward Snowden, the current CIA leaks—they all had indicators that people didn't report because they were friends or colleagues, they didn't want to cause trouble, or they figured someone else would report. Loyalty to their friends trumped their duty to report. They asked, 'What if I'm wrong?' and didn't report."

Self- and proxy reporting are critical to the success of any ITP's detection, prevention, and mitigation efforts. In 2017, the Office of the Director of National Intelligence (ODNI) issued *Security Executive Agent Directive 3* (hereinafter, "SEAD 3"), which mandated reporting of potentially concerning activities. Failure to comply could result in administrative action, including the loss of one's eligibility for a national security clearance.

Given the complexities of human behavior, policy alone will not enable the difficult choice to report. According to behavioral research, people are most likely to make good decisions when they have relevant past experience, have clear information about the situation, and receive prompt feedback (Thaler & Sunstein, 2008). The insider threat indicators that prompt reporting, however, are rarely clear, and few employees outside of security officers would consider themselves practiced reporters. Furthermore, if they do file a report, follow-up inquiries and investigations are sensitive, thereby leaving the employee to trust that the report was actioned fairly, thoroughly, and promptly.

In order to maximize reporting, robust awareness programs that educate, engage, and empower employees must accompany clear policy. At the organizational level, education campaigns must establish relevance so employees clearly understand the link between insider threat behavior and national security. At the individual level, employees must understand what happens once security receives a report in order to help alleviate fears, correct misinformation, and maximize organizational trust.

ITPs must convert employees into allies, and nudge their behavior by making reporting easy (Halpern, 2015). Otherwise, employees may stay silent to maintain the status quo, or avoid any possible stigma attached to a report that turns out to be nothing.

> "A command/control approach to counter-insider threat does not work to ensure long-term compliance. Instead, a person must be inspired to comply by someone he/she respects."
> - *Government SME*

TECHNOLOGY, TOOLS & DATA

"We need to use technology to help us leverage the mass amount of data that are available. Technology can analyze the data faster and better than humans can, which allows investigators to take action sooner. It will help us to intervene sooner."

- *Government SME*

DoD Directive 5205.16, *The DoD Insider Threat Program*, required Components to protect their classified assets against threats posed by individuals who could misuse their authorized access. In accordance with language from the National Defense Authorization Act of FY17, DoD revised 5205.16 in January 2017, and expanded the definition of an insider to include any "person who has, or once had, authorized access to information, a facility, a network, a person, or a resource of the Department."

The sheer size of the past and present DoD workforce, along with the mandate to monitor all activity on classified networks, has motivated a number of technological innovations. Today's user activity monitoring (UAM) and user entity behavioral analytics (UEBA) products can: ingest multiple data sets, to include free text; automatically anonymize data and link datasets; baseline behavior against individual and peer group norms; identify anomalies; assign risk scores; and present actionable results on easy-to-navigate dashboards. Faster processing times and cheaper storage enable agencies to simultaneously gather, organize, and analyze disparate data sets and respond to potential threats in near real-time.

UAM and UEBA tools are expensive, and critics have begun to ask whether the value-add sufficiently exceeds the price tag, especially when these tools have steep learning curves. According to several SMEs, many tools were not designed with end-users in mind, cannot be quickly deployed "out of the box", and/or require maintenance that causes lengthy outages. In the absence of comprehensive and free market surveys, consumers have begun to educate themselves on open source solutions that could meet their needs without the corresponding high cost.

Beyond which tool to purchase is the question of what types of data exist and of those, which provide the most insight into insider threat behavior. As one government SME stated, "No one has a master list of all of the data that are available." Then, once the data sets are identified, organizations must choose what to ingest into the ITP. Agency officials do not want to assume the risk that results from leaving data on the shelf, either because information was never ingested in the first place, or because the ITP Hub did not have enough employees to analyze all of the data.

Insider threat researchers must "not overpromise. There is a unique opportunity to take quantitative data and do something with them. Also, being trusted with very precious datasets means we have to be very careful."

- *Academic SME*

INDIVIDUAL FACTORS

"Research has identified a number of indicators that precede known insider threat incidents, but what are the true differentiators?"
- *Academic SME*

Each year, DoD's Personnel Security Program transforms thousands of outsiders into trusted insiders. Threats persist, however, and to date, no one can answer the most pressing question among ITP stakeholders: who will become an insider threat?

Right now, no one can predict future behavior, and so instead, ITP personnel shift the focus to behavioral indicators that might suggest a potential threat. Many organizations have produced lengthy lists of these indicators, many of which stakeholders can computationally transform into automated triggers. When presented with his organization's own list, however, one government SME asked, "Where did this list come from?" He shared, "I dug into this and got a disturbing answer, which was a few people got together and came up with them. I also did my own research, and the more research I did, the more I learned that there is no scientific background or rationale or reason to some of these indicators." Although anecdotes and experience are valuable, they are an insufficient replacement for empirical research as a foundation for an evidence-based security program.

In addition to behavioral indicators, stakeholders have studied psychological predispositions that may be associated with insider threat behavior in the future. Psychological profiles are rarely available and difficult to collect, but Krofcheck and Gelles found that narcissistic personality disorder and antisocial personality disorder were the most common personality disorders among known spies (as cited in Greitzer, Kangas, Noonan, Brown, & Ferryman, 2014). Research that is more recent suggests that low conscientiousness, high neuroticism, and low agreeableness are the most relevant traits to insider threat because they place individuals at risk for hostility, anger, and stress (Greitzer, et al., 2014).

Although valuable, behavioral indicators and psychological predispositions suffer from the same shortcoming—statistically speaking, they will not resolve to insider threat behavior. From an organizational standpoint, these false positives consume valuable resources because an incident must be put in context in order to be closed. In ITP Hubs, this usually means a follow-up inquiry or investigation.

It may be possible to reduce false positives through rigorous research design. Researchers need to compare cases in which indicators resolved to malicious behavior to those that did not. These comparisons should be prioritized, as they have the potential to get DoD beyond general behavioral indicators to a list of actual differentiators.

"Whenever there is a project that studies administrative and criminal misconduct as a precursor to insider threat, there must be a comparison group. We must compare known goods with known bads."
- *Government SME*

ORGANIZATIONAL FACTORS

"An organization should not delegate its responsibility for building and sustaining organizational loyalty to an Insider Threat Program. The Insider Threat Program must be brought into the boardroom. When leadership takes an active role, it sends the message to employees that they care enough about the program not to delegate the responsibility to others."
- *Industry SME*

In the aftermath of an insider threat incident, many organizations rush to categorize the perpetrator as a bad apple. According to one government SME, however, "What is missing in leaders' minds is the correlation between climate and individual behavior." Most people do not enter an organization with the intent to do harm. Instead, as one government SME stated, "The insider threat is comprised of what a person brings into a workplace and the workplace environment itself."

Insider threat behavior takes place in a social context, and environmental factors can both facilitate and mitigate individual decisions. These factors go well beyond the physical environment of gates, guards, and guns, to include structural policies and cultural practices. For example, zero tolerance policies for bad behavior actually reduce reports of misconduct (U.S. Department of Justice, 2016), while cultural practices, such as a lack of candor in an organization, may enable poor performers to slip through the cracks, or toxic leaders to maintain positions of authority (Paolozzi, 2013). In extreme cases, it may even enable workplace homicide. For instance, rather than separate Nidal Hasan from the military after a pattern of misconduct, he was promoted and transferred to Fort Hood. As an officer informally shared with the receiving officer, "You're getting our worst" (Swaine, 2013).

At the macro-level, organizational trust is vital to employee engagement (Jacobson, 2014) and essential to an organization's success (Shockley-Zalabak, Morreale, & Hackman, 2010). Leaders and security personnel who demonstrate fairness, consistency, and transparency build trust throughout the workforce (Galford & Drapeau, 2003). Among other desirable outcomes, high-trust organizations have a strong sense of shared purpose, and have employees who work together to support that purpose (Hitch, 2016).

At the micro-level, organizations must respond to specific incidents in such a way that does not escalate the situation. As one academic SME noted, "Culture and the people you have in positions that handle the flagged situations matter a lot. You do not want the response to a possible security incident to create an insider threat where one did not exist before."

"Everything you do … must be a structured, supported intervention. . . . If you intervene without support, you just empower a person to become a greater insider threat. If you support without an intervention, the person is sliding through the system, maybe as a ticking time bomb."
- *Government SME*

PROGRAM EVALUATION

"The bottom line for performance metrics is prevention."
- *Government SME*

Organizations implement ITPs to prevent statistically rare events, which makes it difficult to justify requests for additional resources when the current level of effort appears sufficient. As one academic SME asked, "How do we keep organizations on their toes all the time to protect against events that we know will rarely, if ever, happen?"

Absent meaningful metrics, stakeholders and their programs will persist "largely on the intuition of company leadership" (Ohlhause, Poore, McGarvey, & Anderson, 2014: p. 9). Program Managers recognize this challenge, and they have responded by thinking critically about what it means to have an effective ITP. At the most basic level, they measure the success of their processes, such as compliance with the Minimum Standards. Beyond that, they record metrics such as the time it takes to resolve an incident, the number of actionable reports they produce, and the number of times law enforcement reaches back for investigative assistance. Some Program Managers also measure outcomes, such as post-training knowledge retention, the frequency and ease of cross-component communication, and how often employees get back on track after starting down a counterproductive road. As one government SME noted, ". . . what the TMU [Threat Management Unit] does is to gauge a command's return to normalcy. This includes both feelings of safety, and also administrative processes and procedures getting back on track."

As part of a thorough program evaluation, organizations need to be able to benchmark themselves against their peers. To do this, DoD must create measureable standards to ensure valid and reliable comparisons. Taken together, these performance metrics will not only maximize program effectiveness, but will enable the ITP's transition from a cost center to a value center that leadership will want to support (Campbell, 2014).

Finally, as DoD ITPs mature, it will be important to assess the post-compliance landscape. One by one, DoD Components are standing up ITPs that fully comply with federal policy, but how have these programs affected their host organizations? Not all organizations had a security culture prior to Executive Order 13587, and so the introduction of a mandatory ITP represented a significant shift. Successful ITPs should benefit rather than constrain or compromise the enterprise, which includes workforce well-being and retention. Also, ITPs must be positioned to protect against future threats. The threat landscape shifts constantly, and DoD must be able to deploy tools and technologies to prevent threats over the horizon.

"Our Insider Threat Programs are built to protect against Manning and Snowden, but we need to protect against the next threat—the one that hasn't happened yet."
- *Government SME*

STRATEGIC APPROACH

The five campaigns that comprise the SBS Research Plan are the result of a needs assessment, which is the first step in a strategic approach to fully integrate SBS into the counter-insider threat mission space. As the SME interviews demonstrate, SBS research can serve as a force-multiplier to the mandated analytic, response, and training capabilities included in ITPs, but as one industry SME noted, "The challenge for behavioral research scientists is that they will only be as useful as they are allowed to be. This means, in order for behavioral researchers to work, they must be given permission to pursue their research goals." Neither the Minimum Standards nor DoD 5205.16 require ITPs to include a research portfolio. Why, then, would Component leaders endorse and advocate for SBS research, especially when the ITP is an unfunded mandate and resources are scarce?

As part of the interviews, SMEs explained what is required for researchers to continue forward progress and execute the SBS Research Plan. Several SMEs drew on their own experiences building successful ITPs, especially under adverse fiscal and cultural conditions. What follows is a description of the two most commonly mentioned SME strategies for success, and how SBS researchers can leverage these valuable lessons.

TAILOR THE MESSAGE

> "The key to getting access is to build relationships, and in order to do that, Program Managers need to go out and talk with people, identify potential data sources, and explain the program. . . . Personal contact will pique awareness."
>
> - *Government SME*

Like successful ITP managers, SBS researchers must come out from behind their desks to secure the buy-in necessary to execute the SBS Research Plan. Organizational leaders are briefed constantly on initiatives that compete with each other for attention and resources. Similarly, administrators who manage organizational databases receive frequent data requests, and employees are tasked with training that takes time away from their assignments. Program Managers communicate effectively with and build trust among all of these people, and they can serve as a model for SBS researchers. They persuade leaders to prioritize the ITP, administrators to share their data, and employees to report behaviors of concern. They achieve these successes by following one simple rule—Program Managers deliver an informed, in-person message that is tailored specifically to each audience.

One government SME described how he makes threat awareness training relevant to a variety of audiences. He shared, "For a contractor, we talk about revenue and actual technology that has been stolen, if we can talk about it. For a Soldier, we talk about duty and patriotism. . . . We talk about protecting our own people. This isn't an academic exercise."

In order to contribute to the counter-insider threat mission space, SBS research also cannot be an academic exercise. SBS researchers must be able to communicate the operational relevance of their research in terms every audience member will understand, regardless of education or experience (National Academies, 2017). This requires SBS researchers to study actual ITPs (George, 1993). They must, in the words of one government SME, "be seen as problem-solvers" who are able to identify and translate operational challenges into feasible research studies.

Finally, like those who advance technological solutions, SBS researchers cannot overpromise. As one academic SME noted, "Behavioral outcomes always depend . . . Sometimes these gray areas make decision-makers . . . uncomfortable, and this discomfort can lead to disinterest." SBS researchers must manage expectations and communicate honestly in order to preserve both the integrity of the data and the process.

BUILD STRATEGIC PARTNERSHIPS

> "Problems can be resolved when we bring all of the specialists together for a consultation. Everybody's experience comes to the table, collaboratively."
>
> - *Government SME*

Successful ITPs are led by Program Managers who are, according to one government SME, "responsible, professional, committed, and dedicated to their roles. . . . [They are] well-rounded, with a variety of experiences and a working knowledge of several disciplines, including security, Human Resources, privacy, and the Inspector General." The SBS Research Plan cannot be executed by members of one discipline or adherents to one method. Instead, as one academic SME noted, "researchers need to operate and think as multi-disciplinary teams. Insider Threat Program Hubs successfully operate using this teaming model, but this is not yet the case among researchers."

ITPs are built around a whole-person approach, which requires stakeholders from different organizational domains not only to share information, but also interpret the information to resolve a potential incident. As one government SME noted, this can pose significant challenges: "We put security, counterintelligence, law enforcement, and intelligence analysts in the room together and tell them to figure out data, but they do not share a common analytical language or methodology or philosophy or goals." Program Managers successfully bridge these gaps through collaborative working groups, which facilitate mutual respect, trust, and a common language among people who may not have worked together prior to the ITP.

> "We need to learn how to conduct inter-disciplinary policy assessments and how to market our ideas after they have been published. We need to put forth more effort to interact with and brief policymakers and operational personnel."
>
> - *Academic SME*

Under Executive Order 13587, every government agency that operates or accesses classified computer networks must have an insider threat detection and prevention program. In DoD alone, there are now 44 ITPs, one for each Component. Under Change 2 to DoD 5220.22-M, "National Industrial Security Program Operating Manual," all entities that have been granted a facility security clearance also must establish ITPs, which includes private companies, UARCs, and FFRDCs. This collection of diverse organizations offers a number of opportunities for SBS researchers to build strategic partnerships, and in turn, advance the state of insider threat research.

"The Insider Threat Program should be a shared responsibility rather than the exclusive preserve of highly-specialized experts. We must share and collaborate."

- *Academic SME*

CONCLUSION

In the words of one government SME, successful ITPs recognize "the humanity of human behavior"–the messiness, the inconsistency, and the adaptability–and in collaboration with other stakeholders, develop structured and supported interventions for those who may pose a potential threat. Social and behavioral scientists are well-positioned to contribute to this mission space by delivering robust empirical research and actionable, relevant recommendations to guide both policy and practice.

In recognition of the value of this expertise, OUSD(I) partnered with PERSEREC to design an SBS Research Plan and corresponding Strategic Approach to integrate SBS into the DoD counter-insider threat mission space. While this Strategic Plan is the result of a lengthy process, it is just the first step. It represents a consensus view of what is important to address right now according to 66 government, academic, and industry SMEs. The next steps will be to implement this Strategic Plan by engaging with others to educate them about about DoD's SBS capabilities, execute the research questions that operationalize each of the campaigns, and analyze social trends that signal the future of insider threat behavior.

REFERENCES

Campbell, G. (2014). *Measures and metrics in corporate security.* Waltham, MA: Elsevier.

Department of Defense. (2014, Sep. 30). *The DoD insider threat program* (DoD Directive 5205.16(d)). Revised January 25, 2017.

Department of Defense. (2016, May 18). *National Industrial Security Program Operating Manual (NISPOM)* (DoD 5220.22-M). Retrieved from http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/522022M.pdf

Director of National Intelligence. (2017, June 12). *Reporting requirements for personnel with access to classified information or who hold a sensitive position* (Security Executive Agent Directive 3). Retrieved from https://www.dni.gov/files/NCSC/documents/Regulations/SEAD-3-Reporting-U.pdf

Executive Order 13587, *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information*, October 7, 2011.

Galford, R. M., & Drapeau, A. S. (2003, February). Organizational culture: The enemies of trust. *Harvard Business Review*. Retrieved from https://hbr.org/2003/02/the-enemies-of-trust.

George, A. L. (1993). *Bridging the gap: Theory & practice in foreign policy*. Washington, DC: United States Institute of Peace Press.

Greitzer, F. L., Kangas, L. J., Noonan, C. F., Brown, C. R., & Ferryman, T. (2014). Psychosocial modeling of insider threat risk based on behavioral and word use analysis. *e-Service Journal, 9*(1), 106-138.

Halpern, D. (2015). *Inside the nudge unit: How small changes can make a big difference*. London, England: WH Allen.

Hitch, C. (2016). *How to build trust in an organization*. Retrieved from UNC Executive Development website: https://www.kenan-flagler.unc.edu/executive-development/custom-programs/~/media/827B6E285F2141C49D407DF7E5F5A1C4.ashx

Jacobson, D. (2014, February 5). 5 Tips for building trust [Web log post]. Retrieved from http://www.globoforce.com/gfblog/2014/5-tips-for-building-organizational-trust/

National Academies of Sciences, Engineering, and Medicine. (2017). *The value of social, behavioral, and economic sciences to national priorities: A report for the National Science Foundation*. Retrieved from The National Academies Press website: https://www.nap.edu/catalog/24790/the-value-of-social-behavioral-and-economic-sciences-to-national-priorities

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

Ohlhause, P., Poore, M., McGarvey, D., & Anderson, L. (2014). *Persuading senior management with effective, evaluated security metrics*. Alexandria, VA: ASIS International.

Paolozzi, P. (2013, September). Closing the candor chasm: The missing element of Army professionalism. *Professional Military Ethics Monograph Series* (Vol. 5). Retrieved from https://ssi.armywarcollege.edu/pdffiles/PUB1178.pdf

S.2943 Res. 114 Cong. (2017) (enacted). Retrieved from: https://www.congress.gov/bill/114th-congress/senate-bill/2943/text

Shockley-Zalabak, P., Morreale, S., & Hackman, M. Z. (2010, April 29). Organizational trust: A model for building the high-trust organization. *International Association of Business Communicators*. Retrieved from https://www.iabc.com/organizational-trust-model-high-trust-organization/

Swaine, J. (2013). *Fort Hood shooter Nidal Hasan 'left free' to kill.* Retrieved from http://www.telegraph.co.uk/news/worldnews/northamerica/usa/10220449/Fort-Hood-shooter-Nidal-Hasan-left-free-to-kill.html

Thaler, R. H., & Sunstein, C. R. (2008). *Nudge: Improving decisions about health, wealth, and happiness*. New York City, United States: Penguin Books.

U.S. Department of Justice, Federal Bureau of Investigation, Behavioral Analysis Unit – National Center for the Analysis of Violent Crime. (2016). *Making prevention a reality: Identifying, assessing, and managing the threat of targeted attacks.* Retrieved from https://www.fbi.gov/file-repository/making_prevention_a_reality_identifying_assessing_managing_threats_of_ta.pdf

APPENDIX A: SOCIAL & BEHAVIORAL SCIENCE RESEARCH QUESTIONS

SME interviews resulted in five SBS Research Campaigns that together comprise the SBS Research Plan. SMEs also suggested specific research questions within each of the five campaigns. What follows is a list of questions organized by campaign.

EMPLOYEE REPORTING

1. How does a diverse workforce consume security training?
2. How can an organization successfully establish among its employees the link between insider threat behavior and national security?
3. How can an Insider Threat Program (ITP) overcome social ties and cognitive biases in order to maximize self- and proxy reporting?
4. How can an ITP incentivize reporting without encouraging false positives?
5. Who is the most likely to report what they see to an ITP?
6. What types of reportable behavior are most likely to be underreported?
7. What is the most effective medium to enable reporting (e.g., telephone line, anonymous online reporting)?
8. How does organizational trust contribute to employees' willingness to report concerns to an ITP?
9. Which outreach and messaging campaigns have had the most success with regard to increasing employee reporting?

TECHNOLOGY, TOOLS & DATA

1. If an organization acknowledges the use of user activity monitoring (UAM)/user entity behavioral analytics (UEBA), does that affect the frequency of employee self- and proxy reports?
2. What is the cost versus benefit of adding UAM/UEBA to the unclassified network?
3. What technical, operational, and oversight architecture should the military employ for UAM/UEBA in a tactical environment?
4. What are the most effective mathematical and statistical techniques to reduce the number of false positives produced by UAM/UEBA?
5. What is the current state of the market for UAM/UEBA?

INDIVIDUAL FACTORS

1. How does the population of known perpetrators of insider threat behavior compare to the general population?
2. What are the most common concerning behaviors that fall below reportable thresholds?
3. What factors facilitate or mitigate an individual's susceptibility to recruitment by an adversary?
4. How do insider threat behaviors, targets, and motives vary by generation and age?
5. What are the differences between whistleblowers and leakers?
6. Among those who exfiltrate information, how do insider threat behaviors and motives vary by whether the information was classified or unclassified?
7. What are the indicators of radicalization?
8. Which of the dozens of insider threat behavioral indicators are empirically validated versus anecdotally derived?
9. What is the correlation between resiliency and insider threat behavior, and does it vary by whether the behavior involves violence?
10. What is the cost versus value of expanding psychological screening to prevent future insider threat behavior?

ORGANIZATIONAL FACTORS

1. What effect has the ITP had on DoD Components' organizational cultures?
2. How can an organization implement disciplinary action, to include termination, without increasing the likelihood of future retaliation?
3. What valid and reliable measures of organizational climate exist that do not rely on self-report?
4. If an organization adjusted its manning requirements to allow for temporary removals that allowed employees to address stressors that often precede insider threat activity, would it decrease the overall level of insider threat activity?
5. What is the relationship between insider threat behavior and time in service?
6. What steps should an organization take to reintegrate an employee after a closed investigation?
7. Are individuals who access into the Services during recruitment surges more likely to become of record with Insider Threat Program Hubs than those who access during other times?

PROGRAM EVALUATION

1. What performance metrics should be used to demonstrate the effectiveness of ITPs?
2. How can DoD build a reliable and valid benchmarking process for its 44 Component-level ITPs?
3. What is the cost of an ITP versus the cost of an insider threat incident?
4. How does an ITP evolve from a compliance-based effort into a risk-based effort after it has reached full operational capability?
5. What domestic and global trends and events will shape future insider threat behavior?
6. How does insider threat behavior vary by country, and what best practices can DoD adopt from the international community to improve domestic efforts to detect, prevent, and mitigate future incidents?