FY 2021: Strategic Road Map to Leverage Research to Counter Insider Threat

Kelly Jones*, Marilyn Maines*, Ruthanna Gordon,

Michelle Morrison, and Michael Bunting

Applied Research Laboratory for Intelligence and Security

University of Maryland, College Park

May 2020

Please address correspondence to:
Kelly Jones, Ph.D.
Applied Research Laboratory for Intelligence and Security (ARLIS)
7005 52nd Avenue
University of Maryland
College Park, MD 20740
kjones@arlis.umd.edu

*Equal first authors

This document is approved for selective distribution. This living document is the research road map for ARLIS's program on Insider Threat Prevention and is intended to facilitate conversation with ARLIS's government sponsor and customers.

DOPSR Case 21-S-2851

EXECUTIVE SUMMARY

The ARLIS team was tasked with identifying research needs within the insider threat community that drew on its strengths in the social and behavioral sciences, and fully leveraged its position as a University Affiliated Research Center (UARC) serving the US Intelligence Community (IC). Based on an extensive literature review and input from numerous subject matter experts, including our government clients at PERSEREC's Threat Lab, we identified five initial research areas and a strategic approach to our research program for countering insider threat. This Strategic Road Map lays out a path for building a comprehensive, holistic approach to the complex problem of insider threat.

These five research areas include:

1. Moving from Insider Threat to Insider TRUST
2. Investigating Human Behavior Factors
3. Investigating Cultural Factors
4. Investigating Organizational Factors
5. Examining Technical/Cyber Contributions, Including Machine Learning and Artificial Intelligence

This first research area, Insider TRUST, serves as the primary overarching goal for ARLIS's insider threat research program, and provides a foundation for the other four research areas. This approach 'flips the script' – complementing traditional investigative/punitive "detect, deter, mitigate" strategies by seeking ways to build and maintain trustworthy, resilient, and useful systems and teams (Insider TRUST). ARLIS will focus on shifting the paradigm from "right of boom" and the detection of insider threats to "[far] left of boom" and the creation of Insider TRUST.

In support of these five research areas, the ARLIS strategic approach will be to bring its expertise in social and behavioral sciences together with broad University of Maryland capabilities in cyber security and information technology to build a holistic approach to insider threat research.

Two supporting approaches include:

1. Tailoring ARLIS research to a wide range of customer needs
2. Building the ARLIS Hub of Strategic Partnerships with key stakeholders

This Strategic Road Map serves as a starting point for ARLIS research and is a living document that will evolve with the ever-changing threat landscape and to better meet client needs.

Table of Contents

INTRODUCTION: BACKGROUND AND ORIGINS OF THE ARLIS ROAD MAP

Countering threats posed by trusted insiders remains one of the highest priorities for the Department of Defense (DOD) and other US government agencies and organizations. The 2012 National Insider Threat Policy and Minimum Standards (White House Memorandum), along with the 2018 Insider Threat Program Maturity Framework (NITTF), both prompted by Executive Order 13587, provide policies and governance structure for individual agencies and organizations to implement insider threat programs, with wide latitude and variation across organizations. Because "insider threat is, at its core, a human problem that results from a complex interaction among individual and environmental factors"[1] the social and behavioral sciences (SBS) are well-suited to address this complicated and persistent problem.

In 2016, the Office of the Under Secretary of Defense for Intelligence & Security partnered with the Defense Personnel and Security Research Center (PERSEREC) to design a comprehensive research plan for integrating SBS into the DoD counter-insider threat mission space. This plan was developed in collaboration with subject matter experts (SME) and approved by the DoD Insider Threat Program Director in 2018. It 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. In 2019, DoD published a strategic plan for 2020-2024, *DoD Counter-Insider Threat Program Strategic Plan,* including the incorporation of SBS expertise in research and operations. ARLIS's Strategic Road Map lays out the research directions via which we will contribute to solving critical insider threat challenges identified in these foundational documents.

Many Insider Threat Programs today focus largely on using technical tools to detect and monitor potential insider threat-related behaviors among employees. Successful insider threat detection, however, requires a balance between technological approaches and understanding human factors as outlined above. We need enhanced capabilities to detect, deter, mitigate, and prevent threats while also building and maintaining trustworthy, resilient, and useful systems and teams (Insider TRUST).

ARLIS research will increase our understanding of this balanced approach, which we have termed Insider TRUST, including: what factors increase or decrease insider threat and trust; how risks can be detected before harms become irreversible; how organizations can most effectively mitigate those risks or prevent them entirely; and how to cultivate a trustworthy workforce and environment. The work proposed here leverages ARLIS's expertise in the social and behavioral science approaches alongside University of Maryland capabilities in cybersecurity and information technology in a holistic approach to increase our understanding of how to achieve these core goals.

---

[1] Introduction, *DoD Counter-Insider Threat Program Strategic Plan,* August 2019*. pp 8.*

Further, ARLIS is committed to building a consortium to serve as research 'hub' for the insider threat community.

ARLIS STRATEGIC ROAD MAP

RESEARCH APPROACH

The ARLIS team has identified *five* initial research areas for countering insider threat. These research areas are not intended to limit our future directions or paths, but to serve as starting points for further investigation. The goal is for this Strategic Road Map to expand and change with the ever-evolving threat landscape and to better meet client needs.

FIVE RESEARCH AREAS

ARLIS has developed five research areas or paths areas. These are:

1. Moving from Insider Threat to Insider Trust
2. Investigating Human Behavior Factors
3. Investigating Cultural Factors
4. Investigating Organizational Factors
5. Examining Technical Contributions, including Machine Learning and Artificial Intelligence

The following sections provide a high-level view of each research area.

RESEARCH AREA 1: MOVING FROM INSIDER THREAT TO INSIDER TRUST

There has been a recent push in the insider threat community (e.g. CERT, 2018; ODNI, 2020) to "move to the [far] left of boom"—that is, to shift the focus to prevention of volatile situations before they occur by identifying and addressing the chronic [far left] and specific [left] issues that created the situation. Currently, insider threat programs largely use punitive/investigative "Detect, Deter, and Mitigate" approaches, which focus on monitoring and imposing constraints on behavior, as well as detecting and punishing misbehaviors. This is a necessary component but has limitations if used alone because it largely focuses on the "right of boom" factors – in other words the 'after the fact' forensic analysis and prevention of reoccurrence of a similar event. The ARLIS approach will focus on shifting the paradigm from "right of boom" and the detection of insider threats to left of boom" and the creation of "insider TRUST." In order to implement and improve effective programs, it is critical to conduct research that supports a robust balance between these approaches to counter insider threat.

The concept of "Insider TRUST," a shorthand for building and maintaining Trustworthy, Resilient and Useful Systems and Teams (Insider TRUST), could potentially address both the left and far left of boom, by identifying 1) what makes an employee a trusted insider; 2) what makes an employer/organization trusted by its employees; and 3) the factors that can enhance or

undermine trust between individuals, organizations, and systems. For example, trusted insiders and supportive organizational cultures can increase organizational security and resilience, forming a core component of a workforce that is resistant to potential threats. Such a workforce can more effectively identify and manage insider risk by safeguarding national resources, protecting classified information, and defending the safety of colleagues.

The primary goal of this research is to develop the positive or "Insider TRUST" approach – and ultimately to create strategies for reaching this end state. These strategies may include: 1) identifying behaviors and characteristics that indicate trustworthiness in order to foster a core group of trusted insiders who can contribute to the security of the organization; 2) identifying organizational culture that can be shaped to minimize risk and maximize trust; and 3) exploring how to balance approaches in order to develop a holistic, comprehensive approach to the complex problem of insider threat.

This first research area, Insider TRUST, serves as the primary overarching goal for the ARLIS insider threat research program, and provides a foundation for the other research areas. Research areas 2 – 4 focus on applying SBS perspectives to research on insider threat and Insider TRUST. Research Area 5 focuses on the exploring the contributions of cyber and technical perspectives, including machine learning and artificial intelligence, within a human-focused sociotechnical framework.

RESEARCH AREA 2: INVESTIGATING HUMAN BEHAVIOR FACTORS

In order to foster trusted insiders and detect and/or prevent potential insider threats, we need to increase our understanding of the behavioral and psychological indicators of both. Current approaches focus on gathering and analyzing insider threat case studies, identifying common characteristics that could inform detection efforts. However, this case-based approach fails to gather baseline data on trustworthy insiders; thus, it can neither determine the value of the proposed indicators for differentiating the two, nor can it suggest interventions to reduce risk when indicators are detected (e.g., reducing disgruntlement). In order to meet these goals, we need behavioral research that seeks reliable distinctions between trustworthy and untrustworthy community members.

For example, introversion is often listed as a risk factor for insider threat, based on several prominent cases involving introverted actors. However, introversion is extremely common in the general population, with 30-50% of people falling on the lower end of the Extraversion scale[2]. Introversion is even more common in many professions where the capability to cause harm may be particularly high (e.g., computer programmers and analysts[3]). Systematic research could tell

[2] Elleman, L.G., Condon, D. M., Russin, S.E., & Revelle, W. (2018). The personality of US states: Stability from 1999 – 2015. *Journal of Research in Personality, 72*, 64-72. doi: 10.1016/j.jrp.2016.06.022

[3] Gnambs, T. (2015). What makes a computer wiz? Linking personality traits and programming aptitude. *Journal of Research in Personality, 58*, 31-34. doi: 10.1016/j.jrp.2015.07.004Get

us whether introversion is, in fact, more common among malicious insiders than trustworthy ones, but the high base rate means it is unlikely to be an informative indicator.

A better understanding of insider threat and trust requires robust measures of trait and behavior frequencies across the full population of a community. This type of measurement would not depend solely on post hoc examination of insider threat cases but would systematically compare target behaviors and characteristics between trustworthy insiders and those who ultimately harm (or are known to have been prevented from harming) their organizations. Further distinction is necessary between deliberate and negligent harm, and perhaps between even more granular categories (e.g., indicators for violence may differ from those for non-violent threats).

Based on data about a wide range of proposed behavioral indicators, statistical analyses as well as AI and machine learning techniques should be used to identify factors with notably different prevalence across the groups described above, and thus with the potential to distinguish threatening insiders from trustworthy ones. These analyses must consider imbalances in group size, and the risk of statistical noise in small populations such as malicious insiders.

This quantitative understanding of threat/trust indicators would provide a foundation for further behavioral research. The long-term goal of this research area would be to develop underlying causal models for the relationship between indicators and the harmful or supportive behaviors ultimately of interest. Such models have been proposed on an anecdotal basis, describing how insider threats may develop and routes by which they may be mitigated. These could provide a starting point for empirical investigation to determine which evidence-based threat indicators should trigger early intervention and which suggest that changes to an individual's access or employment are warranted, as well as to explore how trustworthiness can be fostered and preserved. Many potential interventions would draw on a better understanding of cultural and organizational factors, described below.

RESEARCH AREA 3: INVESTIGATING CULTURAL FACTORS

In order to develop an effective strategy for countering insider threat, it is necessary to develop a thorough understanding of the sociocultural factors that define the individuals, organizations, or agencies under study and impact the relevant behaviors. This includes an understanding of the identity, norms, values, and perceptual lens that the organization's members hold in common (see Cultural Topography Analytic Framework for more detail[4]), as well as factors that impact the "security culture" of an organization.

"Identity" is the character traits a given group assigns to itself, the reputation it pursues, the individual roles and statuses it designates to members, and the distinctions it makes between

[4] M. Maines, J. Johnson and K. Kartchner, 2018, Cultural Topography Analytic Framework as described in Crossing Nuclear Thresholds, Palgrave-MacMillan, pp29-60.

those people who are considered members of the group ("us"), and those who are not members of the group ("them"). Useful research questions to ask about identity include:

1. Which factors surrounding a given issue would cause individual member's identity to be threatened?
2. Is group cohesion strong along identity lines in response a given issue?
3. What would cause the group to fracture or to unite behind a common front?
4. What individual roles and statuses might group members seek to protect?

"Norms" are accepted, expected, or customary behaviors within a group or organization. Norms can be explicit or implicit, prescriptive or proscriptive. Useful research questions to ask about norms include:

1. Does an issue place social institutions or common practices under threat?
2. To what extent are group norms and preferences in sync with prevailing security (government, industry, academia) norms on an issue?
3. Which practices are likely to be pursued from habit, or bureaucratic inertia, even if out of step with current security practices?
4. Would changes in this policy area (insider threat) offer group members a way out of increasingly unpopular normative practices? Which members?

"Values" are deeply held beliefs about what is desirable, proper, and good that serve as broad guidelines for social life. Values include material or ideational goods that are honored or confer increased status to individual actors or members of groups. Useful research questions to ask about values include:

1. What is considered "honorable" behavior in this group or organization regarding a given issue area?
2. Which local (group) values may conflict with values of a broader cultural (organizational) approach to this issue?
3. Where might value differences between sub-groups groups present an opportunity to determine where cleavages exist?

In addition to the three basic sociocultural factors discussed above, several other factors can impact the security culture of an organization. The first category of factors includes rules and policy of the organization concerning use of technology, social media, and other cyber interactions. Policy changes and introduction of new technical capabilities can impact the established identity, norms, and values held within a group or organization. As mentioned above, culture is unique to not only the larger context (e.g. national, state, local levels), but each organization or agency will have a unique culture and facets that impact their potential for insider threat.

RESEARCH AREA 4: INVESTIGATING ORGANIZATIONAL FACTORS

Literature across domains shows that human behavior results from a complex interaction between the individual and the situation. While most of the research in insider threat has focused on individual characteristics and motivations, far less attention has been paid to the role of the situation and organization. As mentioned above, the recent push to address "[far] left of boom" factors related to insider threat involves identifying and addressing the chronic (far left) and specific (left) issues that contributed to the situation. Organizational factors, or features of an organization or company that are unique to it, such as its culture, policies, or management style, are both far left and left of boom factors. For example, a company policy that is unfairly applied to some workers is likely to create resentment or disgruntlement, while a policy that is fairly applied to all workers is likely to create a sense of trust and justice.

A long history of research in business, management, and psychology has found that cultivating positive work environments is associated with positive outcomes, including increases in productivity, creativity, resiliency, and trust. Conversely, negative work environments are associated with negative outcomes, including burnout, disgruntlement, and decreased productivity. This research offers an array of potential concepts that could be applied to reducing risk of insider threat and cultivating cultures of insider trust. Some preliminary work from SEI CERT (2016) has suggested that these organizational factors could be effective resources to reduce insider threat incidents. Specifically, SEI CERT found that perceived organizational support, which is the extent to which employees believe their organization values their contributions, treats them fairly, and cares about their well-being, was extremely low in several high-profile insider threat cases.

A primary goal of this area of research is to explore the role of the situation and organization in both insider threat and insider trust by identifying relevant organizational factors that could reduce risk from insider threat and/or help cultivate cultures of trustworthy, resilient, and useful systems and teams.

RESEARCH AREA 5: EXAMINING TECHNICAL/CYBER CONTRIBUTIONS, INCLUDING MACHINE LEARNING AND ARTIFICIAL INTELLIGENCE

One of the key findings from the Insider Threat Detection Tools Working Group meeting, held in June 2019 by the NITSIG in collaboration with University of Maryland, was that "Approaches and techniques should be developed for using machine learning (ML) to learn when context is meaningful or explanatory." Current insider threat monitoring technology, which tracks patterns of behavior and indicates areas of possible risk, is limited in its ability to contextualize behavior within the larger picture. The human analysts and investigative teams fill this role, which makes the process time and resource intensive. For example, an employee might log in at an unusual time. This might be a threat indicator, or it might be that the employee is on a business trip in a different part of the world, and determining which is up to the human investigator if the detection tool does not enable such variation. Tools with more sophisticated analytic capabilities, including

machine learning and artificial intelligence, may help take some of the load off human analysts and investigators if designed and deployed well. Several organizations participating in the June 2019 workshop also expressed a desire to understand more about insiders beyond observed behavior, including their intent and motivation, possibly through the integration of contributions from artificial intelligence (AI).

The development of machine learning and AI algorithms for insider threat programs is an emerging area that especially illustrates the need for social and behavioral science and cyber experts to work together. Cyber practitioners provide the expertise to program, deploy, and operate ML/AI algorithms that can help detect, deter, and mitigate insider threat incidents. Social scientists provide the expertise in human behavior, attitudes, and motivations necessary to create algorithms that distinguish relevant behaviors from noise, interpret reports within the larger context, and facilitate effective usage by human insider threat teams. Social scientists can enable teams to better understand the meaning of search results, as well as to evaluate whether proposed algorithms meet their organizational needs.

Deploying ML/AI is potentially controversial in the workforce, as it may be perceived as intrusive, biased, or Orwellian. Social scientists can help develop algorithms that facilitate rather than disrupt workflows, counter human bias rather than exacerbate it, and assuage concerns about their role in building and maintaining insider TRUST. ML/AI algorithms are already under construction or deployed in insider threat programs, and their use is likely to continue to rise, especially as they become more sophisticated and aim to look beyond behavior to understanding context and potentially motivations.

ARLIS is partnering with University of Maryland Computer Science Department, which has a world class research effort on machine learning and artificial intelligence and will convene a stakeholders' conference in Summer 2020 to identify critical research needs and design projects in this area.

CURRENT & EMERGING ISSUES IMPACTING INSIDER THREAT

Though not necessarily a research area in and of itself, the rapid changes in current issues and work environments can create new challenges that are not addressed by existing programs to counter insider threat. Such changes increase the urgency of ongoing, holistic research that can inform responses to new demands, and provide fast answers to new questions. For example, the COVID-19 pandemic has increased telework exponentially, while also increasing employee stressors, reducing morale and group cohesion, and decreasing the visibility of employees to supervisors and to each other. The research areas described above can address many aspects of how these changes affect the management of insider threat and insider TRUST. Some important question that will need to be addressed in the near future include:

1. How does this new work environment change the risks of insider threat?
2. How will the new work environment impact the development of trusted employees and trusting work relationships? How can we appropriately vet potential new employees?

3. How can cyber experts optimally adapt work environments for security when the system is not totally within their control (as people work from home computers and networks)? What legal and ethical issues does monitoring or detection present when occurring in someone's home or on their home network?
4. How will interactions with colleagues and supervisors change when people interact over video calls or instant messaging? How does our interpretation of people's behavior change when presented through new mediums?
5. What value do old predictive indicators (e.g. logging in at odd times of day) translate to the new environment (where people alter their workday to care for family)?
6. What new risk factors do organizations and individuals face (e.g. financial strain)? How do we support our colleagues and employees when they encounter difficulties?
7. For the government and Intelligence Community, how can the mission, which often requires access to classified materials, safely continue while minimizing risks of insider threats and protecting employees' health and wellbeing?

There are many more questions created by the uncertain environment of this pandemic that cannot be addressed by any one expertise, any one perspective, or any one approach. A holistic, integrated research program can create a comprehensive way forward that minimizes risk of insider threats, maximizes trust and resiliency, and optimizes the ability to continue to work under changing conditions.

STRATEGIC APPROACH

These five research areas that comprise the ARLIS Strategic Road Map are the result of literature reviews of community publications and discussions with Subject Matter Experts (SMEs) at key organizations within the Federal Government, academia, and leading contracting and business organizations in the private sector. Development of this Road Map is ARLIS's first step in developing a research approach fully designed to integrate social and behavioral sciences techniques and methods into the counter-insider threat mission space. In addition to these five research campaigns, ARLIS has identified its strategic approach and two additional supporting approaches it will take to building its research program in countering insider threat. ARLIS's strategic approach is the integration of social and behavioral science methods with technical and cyber perspectives into a holistic approach to insider threat. The supporting approaches are the ability to tailor research to a wide range of client needs and the ability to build a hub of strategic partnerships.

INTEGRATING SOCIAL AND BEHAVIORAL SCIENCES WITH TECHNICAL/CYBER PERSPECTIVES INTO A HOLISTIC APPROACH TO INSIDER THREAT

Just as the first research area, moving from insider threat to insider TRUST, serves as the foundation for the other four research areas, the strategic approach serves as the basis for

building a strong research organization for insider threat within ARLIS. Technological and cyber approaches to insider risk have vastly increased in the past decade, especially since the 2011 White House Memorandum mandating the establishment of insider threat programs and implementation of user activity monitoring software on classified systems. A myriad of new, improved, or repurposed technologies have emerged to join long-standing security procedures to address important gaps exploited by several high-profile insider threat incidents. Cyber tools and experts play a critical role in addressing insider threat risks. Cyber experts know the strengths and weaknesses of the information technology system – and how best to defend those systems from a technological standpoint. Cyber tools, when used correctly, impose limits on data movement, user behavior, and access in ways that appropriately minimize risks while maximizing efficiency. Technology will need to continue to evolve as the threat landscape does.

However, cyber tools and experts alone cannot address the complex problem of insider threat because they cannot address elements of the puzzle that are offline or preventative, and because they provide limited insight into the motivations behind detected actions. Similarly, SBS experts and research alone do not address the technical/cyber elements that are key to organizational security. A holistic understanding of insider threat, therefore, requires both social scientists and cyber experts working in concert. ARLIS takes an interdisciplinary approach to research that makes it well suited to lead the way in integrating social behavioral science and cyber perspectives in a comprehensive insider threat research program.

SUPPORTING APPROACH 1: TAILORING ARLIS RESEARCH TO SUPPORT A WIDE RANGE OF CLIENT NEEDS

As ARLIS begins its journey to become a world class research center for Insider Threat and Insider Trust issues, we will construct our program in a way that supports a wide range of client needs, including those of the Federal Government and Intelligence Community, those of academic colleges and universities with research programs in insider threat, and those business organization in the private sector that have experience running insider threat programs to protect their mission and intellectual property. Rather than remaining within the cloistered walls of academic research, ARLIS is a “hands-on” applied research center with awareness of real-world needs and applications. ARLIS products and services will include *traditional research projects* using social and behavioral science techniques and approaches, *test-bed evaluations* for independent validation and verification of insider threat technologies, and *educational outreach and training programs* to support USD(I&S) and IC goals of professionalizing the defense intelligence and security workforce in insider threat. Each of these product areas – research, testbed activity, and training development - will be tailored to meet the needs of the specific customers sponsoring the tasks, but will also be applied, where possible, to support a wider audience in many different formats.

SUPPORTING APPROACH 2: BUILDING THE ARLIS HUB OF STRATEGIC PARTNERSHIPS

ARLIS is well positioned to serve as a hub for strategic partnerships in insider threat research. Taking a consortium-based approach to research, ARLIS has built and maintains strategic partnerships with many key players in insider threat research and operations, including:

1. The US Federal government, particularly the DoD and IC. ARLIS is sponsored by OUSD(I&S), who serves as the senior DoD official for the insider threat program.
2. The University of Maryland. ARLIS, as part of the university, collaborates with other researchers and labs across campus, giving ARLIS a wide range of expertise and resources from which to draw.
3. Other universities. ARLIS collaborates with other academic institutions across the United States, including the DoD HBCU/MI partners.
4. Industry leaders. ARLIS has fostered relationships with industry leaders in this space, including SEI CERT, MITRE, Lockheed Martin, and others.
5. International collaborators, particularly Five Eyes partners. As a first step, ARLIS has fostered close relationships with Australian universities.

One persistent challenge in insider threat is the ability to collaborate and share information, not only across departments within government, but in collaboration with academic, industry, or international partners. ARLIS' consortium model offers a wealth of expertise, resources, and experience that can address the complex problems facing insider threat research.

CONCLUSION

- This Road Map provides direction and core goals for our current research plan and identifies future challenges that we hope to address.

- ARLIS's research approach begins with 'flipping the script' – creating a more holistic, positive "building and maintaining Trustworthy, Resilient and Useful Systems and Teams (Insider TRUST)" approach to complement the traditional, more investigative/punitive, "detect, deter, mitigate" approach to insider threat.

- ARLIS's research will increase our understanding of a balanced approach towards insider threat that focuses on issues "to the left of boom", including: what factors increase or decrease insider threat and insider trust, how risks can be detected before harms become irreversible, how organizations can most effectively mitigate those risks or prevent them entirely, and how to cultivate a trustworthy workforce.

- ARLIS's holistic approach not only focuses on employing established social and behavioral science approaches to increase our understanding of insider threat but

integrating those approaches with cyber/technical ones. This approach also proposes focusing on situational and cultural/organizational factors in addition to the individual factors that play a role in insider threat and Insider TRUST.

- This Road Map is intended to be a living document that is updated and evolves with the ever-changing threat landscape and to better meet client needs.

REFERENCES

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/522022 M.pdf.

Department of Defense. (2019, August 1). DoD Counter-Insider Threat Program Strategic Plan

Elleman, L.G., Condon, D. M., Russin, S.E., & Revelle, W. (2018). The personality of US states: Stability from 1999 – 2015. *Journal of Research in Personality, 72*, 64-72. doi: 10.1016/j.jrp.2016.06.022

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

[1] Gnambs, T. (2015). What makes a computer wiz? Linking personality traits and programming aptitude. *Journal of Research in Personality, 58*, 31-34. doi: 10.1016/j.jrp.2015.07.004Get

Jaros, S.L. (2018) *A Strategic Plan to Leverage the Social & Behavioral Sciences to Counter the Insider Threat* (OPA-2018-082, PERSEREC-18-16). Seaside, CA: Defense Personnel and Security Research Center/Office of People Analytics. DTIC: AD1063771.

J, Johnson, K. Kartchner, M. Maines. (2018) *Crossing Nuclear Thresholds: Leveraging Sociocultural Insights into Nuclear Decision making*. Palgrave Macmillan.29-60.

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-legalreference-book/presidential-memorandum-nitp-minimum-standards-forinsider-threat-program.