Countering Insider Threat (CInT)
(Moving to Insider Risk)
Insider Risk Speaker Series (IRiSS)
Final Report

September 30, 2021

Kelly Jones[1*], Shawn Janzen[1*], Joseph Kelly[1*], Bill Stephens[1], & Adam Russell[1]
[1]Applied Research Laboratory for Intelligence and Security
[*]corresponding authors email addresses: kjones@arlis.umd.edu ; sjanzen@umd.edu ; jkelly@arlis.umd.edu

"I am glad to see the term migrate from Insider Threat to Insider Risk. There are a lot of good reasons for that change, but mostly it avoids unnecessarily alienating the workforce."
– Charlie Phalen, *Principal, CS Phalen & Associates LLC*
Previous Positions
Acting Director, Defense Counterintelligence and Security Agency
Director, National Background Investigations Bureau, Office of the Program Manager
Senior Vice President for Corporate Security, Northrup Grumman
Director of Security, Central Intelligence Agency

EXECUTIVE SUMMARY

Insider Threat is a well-understood concept across the Department of Defense (DoD) and intelligence community (IC) enterprises, even if what constitutes a threat often reflects specific organizational nuances and missions. Likewise, efforts to counter Insider Threat – through deterrence, detection, and mitigation – are also increasingly common topics across DOD/IC enterprises, although reflecting again certain idiosyncrasies of various organizations. Despite these differences, what Insider Threat (InT) and Counter Insider Threat (CInT) approaches generally have in common is the tendency to focus on any given individual as the primary target for efforts to deter, detect, and/or mitigate InT. This paradigm has strong intuitive appeal – of course we want to find the "bad apples" – but has certain limitations when viewed from the perspective of modern environments of growing complexity, where traditional threat-based approaches to finding and neutralizing "bad apples" may be increasingly less effective and increasingly more reactive. This is because our organizations are "sociotechnical systems,"[1] where the complex interactions among different kinds of humans[2], different kinds of technology, and different kinds of dynamic environments mean that the threats, vulnerabilities, and consequences we seek to avoid are increasingly emergent: that is, they emerge from this complex interaction, not just from a single person. Hence, focusing on individuals as "threats" within a complex system will tend to lead us to fixate on characteristics of a given person, and consequently ignore or miss the most important

[1] Sociotechnical systems are characterized by having multiple independent parts, which adapt and pursue different goals in external environments, but which have an internal environment comprising separate but interdependent technical and social subsystems, where goals can be achieved by more than one means and thus require some kind of organizing processes to decide how to achieve goals, and where the performance of the system depends on a "joint optimization" of the technical AND the social subsystems. In sociotechnical systems, focusing on one over the other is likely to lead to degraded performance and unanticipated – and often unwanted – outcomes. By these measures, most DOD and IC organizations ought to be considered sociotechnical systems.
[2] The role of human individual differences and variability means that the challenge of Insider Threat is very much a challenge of the "Human Domain," where advantage goes to the organization that has the best understanding of, and ability to incorporate, human variability, strengths, diversity, limitations, and vulnerabilities into their systems and designs. Achieving this kind of advantage is in part why ARLIS exists to bring its core competencies to Human Domain challenges like Insider Threat.

characteristics of the larger sociotechnical system that can give rise – often unexpectedly – to unwanted behaviors and failure modes.

Other industries also concerned with insider threat have acknowledged this challenge of sociotechnical systems, and many have adapted to the challenge by adopting a "risk"-based paradigm. It is possible that DOD and the IC should also adopt an Insider Risk (InR) paradigm as a necessary supplement to InT, to better position our national security organizations to protect themselves in increasingly complex environments while enhancing their performance.

Briefly, the difference between threat and risk paradigms are summarized in the table below.

Table 1: Comparing the Insider Threat and Insider Risk Paradigms

Insider Threat		Insider Risk
Categorical thinking (threat or not a threat)	↔	Nuanced thinking (degrees of risk)
Static (threats do or do not exist)	↔	Dynamic (risk is always changing based on past & present factors)
Threats must be "neutralized" to be addressed	↔	Risk must be managed since risk can never go to zero.
Focus on the individual as the source of threat, minimal focus on context	↔	Risk comes with interaction of individual, contextual, organizational, systemic, and enterprise variables
People are viewed as the problem	↔	People are part of the solution
Interventions begin largely after concerning behaviors occur	↔	Interventions address identified risks and future vulnerabilities before they can be exploited
	↔	

The primary takeaway from this comparison is one of attention: InT attends to the individual. Seeking to classify individuals as a threat (or not), and consequently efforts to deter, detect, and mitigate InT will necessarily focus on individuals, but often at the expense of considering other key factors. InR, instead, attends to the characteristics of the sociotechnical systems, in which individuals operate, and of which individuals are a key part, but only a part. Concentrating on risk, vs threat, necessarily requires thinking more broadly in terms of failure modes, which is harder but, in the end, potentially much more effective as it incorporates humans and our variability in ways that also acknowledge the importance of sociotechnical contexts in shaping our behaviors.

As part of the effort to explore the value of adopting a risk-based paradigm to complement current InT efforts, ARLIS was tasked to conduct the Insider Risk Speaker Series (IRiSS) under its Countering

Insider Threat (Moving to Insider Risk) contract as part of the ARLIS InR mission area. The IRiSS task was to organize and execute a seminar series bringing together experts and thought leaders to develop an approach to modeling and mitigating insider risk (MInR). IRiSS is part of ARLIS' efforts to build a capability bench to help the US government (USG) deal with emergent sociotechnical challenges and opportunities in complex systems, and draws on its capabilities as a UARC to convene groups from across government and non-government partners, experts, and thought leaders in academia, industry, and non-profits to discuss emerging issues and encourage exchange of new approaches to persistent challenges. Our goals for IRiSS were therefore two-fold:

1. Elicit and integrate diverse perspectives on InT and InR, fostering an environment that leads to better modeling (characterizing, quantifying, predicting) emergent InRs.

2. Elicit and integrate diverse perspectives on InT and InR, fostering an environment that leads to better mitigating (shaping, exploiting, preventing) emergent InRs.

This final report represents the culmination of the IRiSS program which conducted a six-month seminar series that ran from March 2022 through August 2021, wrapping in time to transition cleanly into National Insider Threat Awareness Month (NITAM). The six IRiSS events each carried a different theme and featured different guest speakers—19 in total.

Key session topics:

1. March 2021: State of Insider Threat and Insider Risk paradigms
2. April 2021: From threat to risk: Gain & loss, response, and management around insiders within academic environments
3. May 2021: Industry views – Where are we now
4. June 2021: Tools, methods, and technology -- State of the art in modeling
5. July 2021: Insider risk, human resources, and the human capital supply chain challenge
6. August 2021: Actualizing the Insider Risk Paradigm

Events were well-received by the attendees with strong, positive feedback. Attendance averaged around 200 people per event and almost double that for registration. After six months of engaging InR dialogue with experts and interested individuals, the early reaction to the two goals above posited that we now have good footing to discuss these topics. Through IRiSS and the other InR tasks, we are moving forward with efforts to improve emergent InR models and mitigation efforts. However, such change will take time. In the interim, IRiSS could continue with the popular series, return in a different format, both, explore other routes, or go dormant until needed again.

Table of Contents

INTRODUCTION TO IRiSS

Most of our current and future national security challenges (and opportunities) are emergent – that is, they emerge from complex systems and interactions among humans and different technologies (they are "sociotechnical"). Our historical thinking has been to treat these challenges as complicated - that is, you can break the system into its pieces, understand those pieces in isolation, and then understand and predict the larger system. This kind of thinking lends itself to a "threat" paradigm: where you can isolate (and neutralize) a threat as a standalone "piece" of a complicated system and address it accordingly.

With emergent challenges in complex systems, however, this approach often fails, because analyzing pieces as "threats" will not tell you much about how and where emergent vulnerabilities or opportunities will occur. In complex systems, you need a "risk" paradigm: thinking in terms of where certain risks are likely to emerge and understanding the implications for the larger system as a whole. This requires a cost-benefit analysis that is common in risk-based industries. Moreover, our systems are becoming increasingly interconnected and more complex, so we cannot continue to treat complexity thinking and "risk" as a nice to have if we want to stay competitive and ideally less vulnerable to surprise.

InR reflects sociotechnical emergence: it is (some) function of interactions among different humans and different technologies. Consider that even the most straightforward (though uncommon) scenario - a committed malicious insider who is determined to steal secrets for a competitor. This person who would clearly be a "threat", emerges as a result of that person, the people around them, the systems they have access to, the consequences of their behavior, the systems' defenses, the competitor's own risk tolerance, etc. A committed threat may present low risk to some organizations; likewise, an unwitting person could present unacceptable risk to others.

ARLIS aims to build a capability bench to help the US government (USG) deal with emergent sociotechnical challenges and opportunities in complex systems. Our goals for IRiSS are therefore two-fold:

1. Elicit and integrate diverse perspectives on InT and InR, fostering an environment that leads to better modeling (characterizing, quantifying, predicting) emergent InRs.

2. Elicit and integrate diverse perspectives on InT and InR, fostering an environment that leads to better mitigating (shaping, exploiting, preventing) emergent InRs.

The study and management of risk plays an integral role in physical, personnel, information, and other forms of security and the application of InT paradigms. Yet, much of source and contextual details, modeling options, and solution space nuances are lost when insider as a risk is reduced to insider as a threat. This shift to InR requires substantial reframing from management based on threat elimination toward dynamic situational management where risk is a variable dependent on situational tolerance and requires ongoing consideration for the interaction of individual and contextual variables. This effort emphasizes active decision-making and aids in the measurement of

consequence and risk. People remain a central focus but shift to be part of the solution in helping reduce risk of any kind.

OUSD(I&S) and PERSEREC, as organizational sponsors of ARLIS projects on InT, asked ARLIS to develop a seminar series that would assist in promoting new ideas and perspectives for addressing InT issues. The goal of the series was to help explore a new vision for mitigating InT and to identify ways that further applied research could help the I&S enterprise get closer to achieving this vision.

ARLIS launched the Insider Risk Speaker Series (IRiSS) as a six-part monthly event series with the goal to bring together a variety of great minds to help unpack the challenges and advice of moving from an InT to InR paradigm. Each session featured two to four speakers from different professional perspectives addressing unique session topics and responding to audience Q&A engagement. The IRiSS events kicked off in March 2021 leading up to September as National Insider Threat Awareness Month.

Key session topics featured:

1. March 2021: State of Insider Threat and Insider Risk paradigms
2. April 2021: From threat to risk: Gain & loss, response, and management around insiders within academic environments
3. May 2021: Industry views – Where are we now
4. June 2021: Tools, methods, and technology -- State of the art in modeling
5. July 2021: Insider risk, human resources, and the human capital supply chain challenge
6. August 2021: Actualizing the Insider Risk Paradigm

What is Insider Threat?
Complementary definitions appear in NIST SP 800-53:

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

– *NIST SP 800-53 Rev. 4 under Insider Threat Presidential Memorandum, National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs*

"An entity with authorized access (i.e., within the security domain) that has the potential to harm an information system or enterprise through destruction, disclosure, modification of data, and/or denial of service."

– *NIST SP 800-53 Rev. 4 under Insider Threat CNSSI 4009*

"…thank you for your passion and your ability to bring together fantastic speakers and community engagement around Insider Risk. Your choice of topics and speakers are really strong and aligned with [… delete company name] vision of Insider Risk and our desire to further educate the security community."

Speakers came from a range of government, industry, and academic communities. This series benefitted from this professional diversity, offering novel insights to challenge new thinking for the development of InR management and modeling within the security community. Interest areas included the advancement of enterprise risk management concepts for impact, risk equations, and the use of AI/ML and social & behavioral sciences for quantifying and managing risk.

This series helped foster discussion within events, but also continue post-event through online engagement via publications that capture concepts discussed and community points of interest raised. The triangulation of topics throughout the series and ongoing communications sought to compound to promote the paradigm evolution from InT to InR. This speaker series helped prepare and encourage the security community for robust conversations on InR in time for National Insider Threat Awareness Month.

The speaker series was a public event, open to all that registered. The audience comprised largely government, industry, defense industrial base (DIB), research personnel working on InT programs, as well as academia, nonprofits, and others in the policy space. The security community further benefitted from the broad audience representation during the Q&A portion as well as help extend professional networks, which in-turn may improve the depth and reach of developing new capabilities for InR management.

PROGRAM SUMMARY

This section provides a high-level overview of the IRiSS program as a whole and then discusses the individual events and lessons learned from those events. The program summary is followed by a program evaluation, next steps, and finally a series of appendices for supplemental information. Appendices of interest for this section include Appendix 1: Speaker Bios, Appendix 4: Event Question Lists, and Appendix 5: Event Summaries.

IRiSS was a task developed to help define program goals around InR in support of Objective 1 of the Countering Insider Threat (CInT) Moving to Insider Risk Contract. Task 0 was charged to organize and execute a seminar series bringing together experts and thought leaders to develop an approach to modeling and MInR. A Task 0 team assembled with a coordinator performing most of the day-to-

day operations, led by the CInR Co-PI, and regular guidance from the rest of the CInR leadership team. Task 0 branded the series as the IRiSS.

The speaker series events supported the first InR mission objective, to shift the paradigm from InT models to an InR paradigm. To meet this objective and bolster a lasting evolution, this work required expertise with respect to operational, technical, and cultural changes that can help the USG and its stakeholders. The IRiSS team convened speaker panels to access that expert knowledge, as well as fostered a growing community of individuals and organizations that are that the very least, interested in the paradigm shift.

While grammatically, the change is as simple as a word substitution from InT to InR; in practice, the difference is so much more conceptually and perceptually. It requires revaluating thoughts and practices once thought commonplace. Although each IRiSS event had a different theme and question list, every speaker contributed toward a growing body of knowledge that helps the overall shift. Threat-based approaches tend toward neutralizing identified threats, an increasingly problematic approach given the binary nature of threat identification and non-binary, complex, context-rich people living in equally dynamic environments. The IRiSS team recruited speakers based on their diverse range of leadership, place within their organizations, professional expertise, individual diversity, and with consideration of their positions on the paradigm shift.
Six events took place between March 2021 and August 2021. Most events had a two or three-person speaker panel, and ran 60 minutes, with half of that time dedicated to answering questions sent in advance to the guest speakers and used the remaining time for open question and answer (Q&A) with the event attendees. The first and last events, a kickoff and capstone respectively, followed similarly with the exception that they ran 90 minutes and had four speakers on the panel. The IRiSS coordinator served as the event moderator at all events, while other members of the IRiSS team assisted events with notetaking, meeting introductions, and recruitment, and other logistical support.

Following each event, team notes became non-attributed summaries and contained takeaways useful for addressing various parts of the paradigm shift effort. What follows is a review of each IRiSS event and the takeaway from that event.

#1: State of InT and Insider Risk paradigms

The first event was a kickoff event, designed to get an initial grounding on the InR topic and learn to what extent the first speaker panel would agree or disagree with the premise that a paradigm shift is necessary. The speaker panel comprised of Doug Thomas, a former federal bureaucrat with deep expertise in the intelligence community and InT and InR who now directs similar efforts in the private sector. Dr. Natalie Scala is an academic with expertise in physical and cyber InTs for election polls, as well as decision analysis and experience working with government clients. Matt Eanes directs PAC PMO, helps lead traction on Trusted Workforce 2.0, and works to advance the Federal governments' personal vetting mission. [4th speaker name redacted] leads InR at [company name redacted] and helps protect [company name redacted]'s people, property, customers, and

reputation. This event was different from those that follow, in that the speakers were divided into groups where they could address areas more to their expertise and then reconvened at the end of the first portion for final questions before transitioning to the open Q&A portion.

The overall themes that emerged pertained to issues of complexity that are inherently built into the human domain, which, in turn, affects our current metrics for effectiveness, and the need to foster individual and team support within an organization. The paradigm shift from InT to InR is not just a wording change or looking at a different type or source of data. The shift is also a narrative change that requires empowerment, trust, and sociotechnical solutions without being singly reliant either on people or technology. Yet even a full pivot to InR may not be sufficient to maintain security for our people, organization, customers, and sensitive, proprietary, and intellectual property. InR is a good, next step from InT but not the final one. The values and measures needed to continue this evolution will require ongoing conversations and research as we move the dial from problems to solutions. As we look to the future, many contributing norms and values, such as those related to privacy, will continue to affect InR work, but the degree to which those norms and values continue to contribute may largely depend on their changes over time.

This event set the tone for the rest of the series and was widely lauded as a fantastic start. The kickoff speakers did not directly address InR modeling or mitigation per se, in accordance with the IRiSS Task 0 objectives. However, these speakers set a crucial foundation upon which the rest of the series would build as we seek to answer the task's objectives. Moreover, their takeaways identified the paradigm shift not so much as a single step, but rather an evolving system, complete with opportunities for change and key individual and organizational perspectives from which we can already look ahead to Insider Trust, which directly relates to another task in the ARLIS InR mission.

#2: From threat to risk: Gain & loss, response, and management around insiders within academic environments

Coming off the thrill of a successful first IRiSS event, the IRiSS team featured a topic very close to the UARC given our connection to the university research systems, as well as no shortage of news headlines regarding faculty at well-established places of higher learning finding themselves in trouble for violating InT, InR, or other security policies. The second event focused on understanding how engaging with InT and InR is fundamentally different within an academic setting compared to a non-academic or even a research-intensive experience.

> "The series looks so interesting. Could you keep me in the loop for further discussions? Look forward to learning about your efforts going forward."
>
> – *anonymous*

This IRiSS event brought together two experts from the academic setting, from different but complementary sides of the research enterprise. Dr. Laurie Locascio is the Vice President for Research at two of the University of Maryland campuses. In addition to being a full professor and coordinating strategic research partnerships, she oversaw $1.1 billion in external research funding. Dr. Kevin Gamache coordinates his work as Chief Research Security Officer across 11 campuses of the Texas A&M University System and is also a professor. Additionally, Dr. Gamache established and leads the Academic Security & Counter Exploitation Program, an association of U.S. universities established to help heighten security awareness in academia.

"Changes from threat to risk occur through intentional and actionable inflection points that work best as ongoing, supportive, and inclusive initiatives at the organization's grassroots level."
– Event 3: Industry Speaker

"External relationships with government partners are critical, mutually beneficial, and evolving as we learn from each other; and unlike government and industry relations, copy & paste best practices does not work."
– Event 2: Academic Env. Speaker

The attendees were highly engaged, and the speakers largely agreed with each other, building upon each other's detailed responses. Lessons learned include that collaboration between the research community and security remains a great challenge and natural friction source. More and better risk/impact data can help bridge difference in priorities between these groups. External relationships with government partners are critical, mutually beneficial, and evolving as we learn from each other; and unlike government and industry relations, copy and paste adoption of best practices does not work. Also, when InR programs are working well, they are like a good cybersecurity program: invisibly running in the background, but massive failures can result in lasting damages to an ability to innovate at individual academic, university, and national levels

This event was useful toward the series overall, in part because it revealed that even with a perfectly designed InT program, there are inherent situated features of the academic environment that will naturally resist such security controls. This resistance is not malicious or even necessarily accidental, the two default views for most InT individual identifier labels. Rather, the natural friction stems from differing missions and cultural systems and the values therein. Thus, better mitigation of emerging InRs can start with actively seeking a better understanding and acceptance of these natural friction points and using cultural change cues to improve InR education, buy-in, and compliance. Meanwhile, turning an eye externally, academic environments need positive relationships with outside partners with government and industry; both sides of that partnership benefits from understanding more about the nuances faced by security professionals within academic environments.

#3: Industry views – Where are we now

Cycling from one sector to another was the next stop on the experiential tour, destination private sector. To help identify and advance 'best practices' from industry, the IRiSS team sought out experts who could identify the latest InR advancements in their companies and what they see as must-dos for shifting the paradigm.

Two experts on the cutting edge of InR joined the panel—Stephen Szypulski and Caroline Gilman. As VP of Goldman Sach's Global Compliance Division, Mr. Szypulski brought domestic and international views to the virtual table. His InT program exists within compliance structures, rather than the traditional security, risk management, or information technology corporate structures. At a similarly large firm, Ms. Gilman runs Booz Allen Hamilton's Insider Risk Management Program and brought her expertise in securing people, data, and operations internally, as well as consulting on the same for clients. Rounding out the speaker panel was Dr. David Mussington who contributed extensive expertise working alongside both government and industry, most recently with his new position as CISA's EAD for the Infrastructure Security Division. Much of his previous work focused on training and risk of cyber-physical systems and risk assessments—key areas needed to improve understanding risk models.

The panelists readily provided insights from their own organizations as well as experience gained through collaborations. This open exchange fostered a highly interactive session. Even when the speakers did not agree on a given topic, areas of overlap were apparent which suggested common approaches are possible. Lessons learned included that industry is generally good at understanding risk widely, so thinking about InR as part of the larger risk ecosystem allows use of a wider range of management tools, practices, and perspectives. Changes from threat to risk occur through intentional and actionable inflection points that work best as ongoing, supportive, and inclusive initiatives at the organization's grassroots level. Also, some of the best actions are designed to be pre-emptive: sharing examples of good outcomes, strengthening leadership support and partnerships with government and across industries, expanding equity, diversity, and collaborative professional programs within the organization.

Placing this event, interaction with the speakers, and the takeaways alongside Task 0's two objectives, a few lessons emerge. Obtaining better models that can characterize, quantify, or predict emergent InRs requires being intentional, actionable, and pre-emptive. Furthermore, efforts to mitigate emergent InRs must account for contexts within the larger risk ecosystem. While this could complicate risk mitigation work, as well as attempts to form better models, such work should also be able to leverage other risk management tools to assist in mitigation and support identifying useful models for the better models.

#4: Tools, methods, and technology – State of the art in modeling

With an intentional event topic road map underway—foundation, academic environments, and industry views complete—it was time to turn IRiSS attention to the tools, methods, and techniques that InR programs rely upon. This event directly addressed the first Task 0 objective.

Keeping with the three-speaker panel model, this event featured Katherine Hibbs Pherson, whose tenure at the CIA, other public service organizations, and current consulting firm not only put her on the cutting edge of security and intelligence risk modeling, but also elevated her to influential leadership positions that guided risk modeling practices across government and industry. Lead Insider Threat Researcher Andrew Moore of the CMU Software Engineering Institute brought his sociotechnical analytical prowess to the panel, leveraging an equally lengthy career in research and application of risk methods, models, and tools on systems that keep our critical technologies safe. Jeffrey Dodson, brought balance to the panel with his expertise at the executive level and macro views of decision making for risk management and assurance, informed by his work as Chief Security Officer at BAE Systems and on the ND-ISAC Board.

> "**…**everyone working on Insider Risk should be a modeler, with some degree of conceptual to technical…"
> *– Event 4: Modeling Speaker*

This session spanned a wide range of InR modeling topics, and the attendees did not hold back with their desire to learn more from this expert group. Much of the focus pertained to successful modeling, understanding what is good, obtaining and adapting new information into models, communication, and understanding boundaries and challenges. Lessons learned included that everyone working on InR should be a modeler, with some degree of conceptual to technical capability. Understanding boundaries on risk conditions and acceptable loss informs discussion of what will be acceptable risk, and this is best guided by leadership. We should broadly seek out new information for models across disciplines, sectors, and media formats; seek to bridge the three investigative tracks – HR, ethics, and security and be inclusive throughout the organization. We need to focus less on the individual, more on context; less on process, more on outcome; less on easy but less valuable models, more on thoughtful model design and sources of information.

You would not be in the minority to assume that you would get deep in the weeds on actual model building and variable selection and testing at a session specifically on the state of the art in modeling. Yet, the speakers kept the kept most of the conversation high enough that most lay people could follow along on how to improve their work. The surprise twist of this session, which spoke to the first Task 0 objective to better model emergent InR, came in the stunning amount of speaker agreement on where to direct attention to be thoughtful about model design. They effectively echoed for broad understanding, the necessity for including context in models, that people matter, and ideas of iterative work for nuanced outcomes rather than allowing for more checks on a checklist and defaulting to heuristics and intuition driven decision matrices.

#5: Insider risk, human resources, and the human capital supply chain challenge

Having a session on InR and workforce challenges seemed like a natural fit to follow the modeling session. However, the industry and modeling panels took this to the next level, setting this session up with messaging about the importance of understanding and focusing on the human elements, that greater focus needed to be on the system and the context, and that organizations must be deliberatively collaborative, supportive, and diverse.

Picking up on these proverbial appetizers, the fifth speaker panel has more than 100 years of related experience between them. The panel included Charles Phalen, currently with his own consulting company, drew upon his vast experience with over 40 years of vetting and security work across the federal government and industry that could fill pages. ARLIS's own Professor of the Practice, LTC (ret.) Heather McMahon, implemented and studied intelligence, security, and risk at every level from platoon to senior executive and helped examine risk and workforce challenges in the military. [3rd speaker name redacted] serves as [title redacted]—a division that grew from [company name redacted]'s first InT program that he designed.

> "[Countering InR] issues remain sociotechnical in complex, multidimensional systems, there was a recuring interest to reduce our reliance on technology—there are no technological silver bullets that produce ground truth."
> – *Event 6: Capstone Speaker*

This panel firmly outlined that a successful InR program does not operate in a vacuum and accounts for the whole workforce lifespan from hiring to separation. This becomes increasingly apparent during periods of hiring and continuous vetting. Such processes benefit from deliberative, proactive, collaborative engagement between HR, legal, security, employee relations, and other relative departments and stakeholders. Moreover, this engagement should have buy-in from top leadership and be useful to help develop an organizational culture of security and reduce workforce alienation. InR, hiring, vetting, and other workforce processes should adapt to account for social and technological changes. Collaborative planning and being intentional, such as recognizing the need for increased diversity, can offset adaptation difficulties. Obtaining useful information for hiring and continuous vetting remains a major challenge, which is social rather than technical, despite access to potentially large amounts of information, such as online activity; however, artificial intelligence and machine learning (AI/ML) may offer sorting solutions. Many opportunities remain in the workforce supply chain and InR nexus which can be leveraged through collaborative planning, early intervention, and intentionally improving trust within the organizational culture.

> "Obtaining useful information for hiring and continuous vetting remains a major challenge, which is social rather than technical…"
> – *Event 5: Workforce Speaker*

This event scaffolded core guiding takeaways that could help better mitigate emergent InRs, satisfying additional progress toward this Task 0

objective. Pathways to mitigate InR could be heard in responses to nearly every question, but key focal areas include taking a whole lifecycle approach to understanding employees, being intentional about collaboration and doing so widely across departments, and, along with good leadership, (re)shape organizational culture as a meaningful solution for inclusion and diversity—key elements that may sound very familiar from the industry views session (Event #3).

#6: Actualizing the Insider Risk Paradigm

The capstone event sought to shine a spotlight on the previous five-month journey through well-received topics. Unlike previous events where speakers answered key questions, the speakers provided reaction-style comments to key takeaways from the previous IRiSS events which were provided in advance; along with the usual time for real-time questions posed by the event attendees. Like the kickoff event, this session was the longer 90-minute version and featured a fourth panelist.

This final panel comprised of [1st speaker name redacted], [title and company redacted], who oversees policy, resources, and authority for a substantial among of security and other operations that keep the US safe. InT and InR are daily topics with her duties. Robert Rohrer, as the NCSC's AD and NITFF's Director, leads the very offices that help make the NITAM possible and he drew upon his deep background in criminal and national security investigations. As Director of Security at GDIW, MJ Thomas oversees the entire security enterprise, and called upon her previous work with investigative leadership at the FBI and their Senior Advisor to the DoD. Last but surely not least, ARLIS's own Professor of Practice, LTG (ret.) Darsie Rogers leveraged his expertise leading adaptable and high performing teams who by the nature of their profession operate in high risk, high stress environments.

Overall, the speakers largely agreed with previous takeaways and expanded on them. Major focus areas included a heavy emphasis on good leadership and recognizing the interdependent relationships between security, counterintelligence (CI), human resources (HR), and other departments with recommendations for increased collaboration. Organizational culture and the importance of trust and positive, empowering environments play an important but underused role in Counter Insider Risk (CInR) programs. Echoing throughout the entire session, CInR programs have a dual role as supporting and being supported by people. As such, speakers firmly rooted CInR as human security and identified individuals as the most important focus, juxtaposing to the modeling event takeaway. While these issues remain sociotechnical in complex, multidimensional systems, there was a recuring interest to reduce our reliance on technology—there are no technological silver bullets that produce ground truth. Other key interests included strengthening security and InR efforts by tying them to funding and baking security into contracts with clear consequences. Speakers admitted we have much still to do and acknowledged this event as a robust discussion focused on the right direction.

This dynamic panel demonstrated both how they generally agreed with some speakers but not so much with others on key takeaways. They provided rationale, examples, and analogies where they differentiated from previous event takeaways. Hearing this mix of agreement and dissent with previous speakers offers a gateway opportunity for future work to either bring back speakers with

differing opinions to see how their reactions can drive conversations forward or revisit these topics with additional speakers to see where the consensus lines form and what we can learn about them as they relate to the InR paradigm shift.

PROGRAM EVALUATION

While ARLIS has hosted events of varying size and conducted speaker series, IRiSS was the first of its kind for ARLIS in the mitigating InR mission area that was both intentionally free to attend, public-facing and keyed to a single, ongoing topic: InR.

A brief review of the IRiSS considered three core areas: program development and outreach; event performance; and post-event review.

Program development and outreach

The IRiSS team met weekly to discuss all aspects of the speaker series, and by email as needed. This communication flow worked well to help establish this program from the ground up. There was active planning to select and invite the speakers for each session, which worked well given the overwhelmingly positive feedback received about the speaker panels and topics discussed. Program development and planning feedback was solicited from ARLIS leadership and the program sponsor.

ZoomGov was the event platform for IRiSS, as was the integrated registration system. Pre-registration required submission of a name and email address. Registrants also had the option to share their organizational affiliation through an open text field. Once an event was live, registrants had direct access to the event rather than wait for a confirmation email. IRiSS coordinator, Shawn Janzen, and ARLIS Outreach and Event Specialist Rick Phillips handed troubleshooting when individuals encountered registration challenges. While an exact record log of such issues was not maintained, Shawn Janzen estimated there were perhaps 14 individuals that needed help. Most of this assistance pertained to the lack of ZoomGov accessibility at the individual's organization. When applicable, a DOD memo[3] was shared with the individual in support of gaining access to ZoomGov.

Outreach efforts was predominantly conducted via UMD email, supported in combination by the Threat Lab listserv courtesy of Ms. Stephanie Jaros, colleague networks, and previous event attendee registration lists. The events were also posted to LinkedIN and Twitter, although traction here was limited because the series design overall did not include marketing plan support.

Recommendation: If there will be future activity, retain the contacts made with this program and

[3] The DOD memo did not have a document number, but the subject was "Authorized Telework Capabilities and Guidance", dated April 13, 2020.

incorporate them into future outreach. Do not recreate the wheel. Improve on the communication tools to use a more robust system appropriate for messaging at scale.

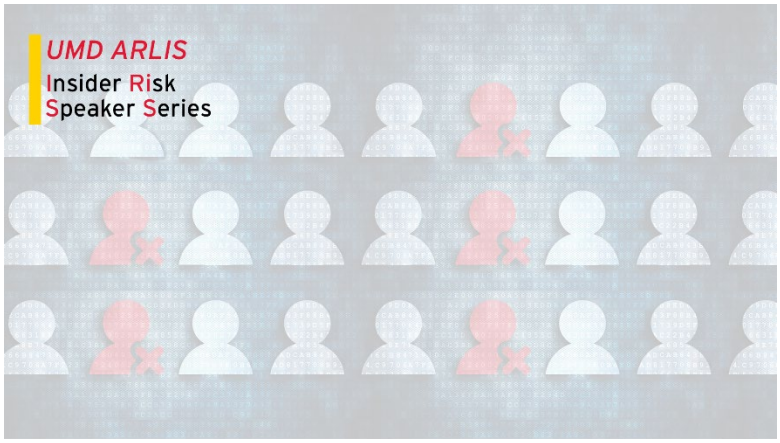
Event performance

Event performance could be summed up with one question. Did the show go off well? The short answer was yes, absolutely yes. The longer response addressed more of the user experience and implementing the IRiSS sessions, reported as understood by the IRiSS Coordinator and informed by feedback and other details available in Appendix 2.

As noted above, there were occasional issues with individuals being able to access ZoomGov. Most of the time, by the event day, these issues were either resolved, an alternative access found, or the individual opted not to attend. Occasionally, the IRiSS Coordinator received an email, perhaps four of them over the course of the whole series, sent while an attendee tried to log into the event, but those emails typically arrived by the time the coordinator was already moderating the event and unable to read the email, much less reply with guidance. The coordinator would email the individual after the event to ensure there were fewer challenges next time.

> *Recommendation:* Assign an IRiSS team member to cover login issues during the event. This may require either having a secondary email / POC listed on the event materials or have someone other than the coordinator moderate the event so that the coordinator can respond to login issues.

Figure 1: IRiSS Team Virtual Background



As a platform, ZoomGov performed rather well. The interface was simple to control, and the features were able to meet all necessary requirements, such as camera and microphone restrictions, waiting rooms, and options for virtual backgrounds.[4] The IRiSS team opted to use a standard ZoomGov meeting room over a webinar meeting, because the regular room allowed attendees to openly chat with all others, whereas webinars restricted attendees from communicating with each other during the session. Open chat access was a key design element for this series to help build a community around this topic space. Only once was there a very minor incident where an attendee's microphone was off mute, which led to radio noise over the speakers; however, the situation was quickly remedied. Zoom's waiting room feature was also an essential feature that worked very well for event-day prep with the speakers before the session started. None of the speakers offered any comments about the

[4] Virtual backgrounds allowed for IRiSS team members to use a special IRiSS event background, see Figure 1.

ZoomGov platform choice, and audio & video quality was as good as any other platforms, or better, as discussed by the IRiSS team. Unfortunately, the longer attendee survey did not go at initially planned, and so the IRiSS team does not have data to see if/how attendees faired with the quality of their user experience.

> *Recommendation:* None immediately for platform review. Plan for how this system can be used better with events moving into hybrid formats, should that format be adopted for IRiSS.

Moderating two-to-four speakers and monitoring hundreds of attendees at once was possible because of the virtual environment. It would have been far more difficult to conduct the same level of engagement in-person, although it would have come at the tradeoff of any post-event small talk. Allowing attendees to post questions to the chat enabled the coordinator to copy them to another document and triage them before he conveyed them to the speakers. More on this point in the next steps section of this report.

> "...The ARLIS institution has become one of my preferred organizations for authoritative information and experts on insider risk and other security topics. As a Marylander, it's great to know that UMD is the USG's applied research lab in the field of intel and security."
>
> – *anonymous*

Post-event review

This portion contains analysis covered in Appendix 2.

Although talking about InT and InR issues in a public, open, and unclassified forum was unlikely to attract wide public attention outside the existing InT community, it attracted very well-known and experienced expert speakers and an engaged an audience for six months. Additionally, given this was the first event of its kind at ARLIS in the InR mission area, the post-review results are very good. For the purposes of event analysis, most tracking was done through a combination of email address and name inspection along using registration and attendance logs generated by ZoomGov. Sector identification classified individuals as affiliated with a government, academic, private / nonprofit organizations, or unknown; a phone classifier was initially a subclass of unknown but later made into its own category due the quantity of phone numbers. This was manual classification through visual inspection of email address domains and provided organization names.[5] The government group included both military and civilian organizations, and did not distinguish between tribal, local, state, federal, and international levels of government.

As the data was processed, some organizations used a non-US domain email address and/or identified as part of a foreign/international government or company. While this facet was not deeply explored regarding differences that exist between US and international counterparts with respect to

[5] Classification errors may exist through unfamiliar organization names or when a group mismatch existed between email address and known organization type, such as a university email but a government agency organization name. This may occur when a person has multiple affiliations and the group code only allowed for a single classification.

IRiSS, a short list of identified international organizations appears below. Most occurred only once but a few appeared as often as three times in the data.

Table 2: Attendee Organization Affiliation by Group

Group	# Attendees	% Attendees
Government	437	34%
Private / NPO	553	43%
Academia	163	13%
Phone	130	10%
Unknown	17	1%
Total	1300	100%

Example foreign organizations represented by IRiSS attendees:

- *Government:* NATO, SciPol, New Zealand Defense Force, British Defense Staff, UK Cabinet Office, UK Ministry of Defense
- *Academia:* University of Oxford, University of Johannesburg, Carleton University, Bournemouth University, University of Warwick
- *Private / Nonprofit:* ABSA Group, Camor, Canadian Nuclear Laboratories, Pramerica

Event registration and attendance across six events averaged 365 and 210 people respectively. Turnover, when a registered person attended the registered event, was often the high-50 to low-60 percent margin, higher than the expected 50% for free, online events. The IRiSS team expected USG representation to be the largest portion of the attendees; and yet it turned out to be people associated with profit / nonprofit private organizations by a seven-percentage point margin. Academia and unknown groups landed within the anticipated range. See Tables 2 and 3 for more data, as well as Appendix 2 for even more tables.

Table 3: Participation Overview

Event	RSVP	Attend (w/o phone)	% Attend (w/o phone)	Attend (+ phone)	% Attend (+ phone)
#1 Kickoff	468	221	47%	246	53%
#2 Academia	380	195	51%	231	61%
#3 Industry	281	165	59%	183	65%
#4 Modeling	407	183	45%	207	51%
#5 Workforce	315	176	56%	194	62%
#6 Capstone	338	171	51%	202	60%

One number stuck out as perhaps both the most exciting value and yet also the one that signaled the greatest room for improvement: 1,300. This was the number of unique persons, interested to register and/or attend IRiSS events. Granted, 10% of this value was unique phone numbers, and since some of those phone numbers were individuals calling in because they cannot connect to audio from their computer, the actual unique persons value was likely a bit lower. Even still, breaching well beyond a 1,000-person ceiling for the entire series was a testament to the program, the program planners, speakers, and attendees. Yet should the IRiSS program continue with another iteration, the 1,300 number will be one of IRiSS' greatest challenges for the future. This placed around 14-19% of these individuals having attended an IRiSS event together. This means that while IRiSS likely had, and may continue to be, developing a core of interested individuals, most of them

were only attending one or two events. There was room to do better, but the foundation was there as seen in the feedback.

Feedback came through feedback polls conducted at towards the end of the session for both events 5 and 6. It also arrived unsolicited as email or event chat comments. The polls provided limited quantitative insight to several measures of overall satisfaction, while the written feedback helped illustrate the poll results. Tables with the poll results appear in Appendix 2.

Table 4: Satisfied (4 or 5)*

Overall Satisfaction:	Event 5: Workforce	Event 6: Capstone
Met Expectations	95%	90%
Topic Quality & Organizational Relevance	95%	88%
Advance Conversation in Their Community	88%	78%
Speakers & Overall Engagement	96%	93%

* *Where 1=Terrible and 5=Excellent*

The poll results from both events were largely positive. Participation was around 42% and 24% respectively and seemed rather close to being representative to the distribution of organizational groups.[6] Of 124 respondents over two events with eight satisfaction questions (four of them asked twice), only one of the 992 total responses was rated two and none were rated one out of five, where one is terrible and five is excellent. Conversely, six of the eight questions consistently scored Excellent among 59% or more of the respondents. Moreover, combining the number responses that gave a 4 or 5 score together, which accounted for 93% and 87% of the event 5 and 6 responses respectively, most satisfaction measures hit 88-95% approval. The lowest was the capstone event's 'advancing the conversation it the community' measure with healthy 78% of the 41 responses responding with either a four or five.

Since the open feedback came unexpectedly and intermittently, a suitable comment tracking system was not developed and implemented. All open feedback was treated anonymously for this program. Thus, matching open feedback to useful measures such as organization type was not done; however, this is an area for improvement on future work. The team received 23 individual comments, all positive. They ranged from the shorter and simpler 'thank you' to naming, at least in part, how or why the IRiSS work was meaningful to that person. The primary takeaway from the open feedback was to keep doing what we are doing, that it is all highly appreciated. A list of the open feedback received appears in Appendix 3.

It is worth mentioning that the IRiSS Coordinator received regular questions if the events were recorded and were made available after the event. The IRiSS team deliberated decided to not record the IRiSS events for the express purpose to foster a more open and candid environment for both the

[6] They are not statistically different. Chi-Square Goodness of Fit results are in Appendix 2.

speakers and attendees. To further promote this, at the beginning of each event, the coordinator shared the house rules which included no direct attribution of anyone attending the event.

The no-recording decision had positive and negative impacts on the IRiSS program. On the positive side, there was robust conversations in most of the IRiSS events via the ZoomGov chat. Although there was no counterfactual to determine if the chat would have still occurred, the IRiSS team found greater value in erring on the side of caution to maintain the no-recording policy. Yet, choosing to record can have had negative impacts. A side effect of recording an IRiSS event may have encouraged lower attendance rates. Even a highly interested person may have opted for the video portion if they had high demands on their availability during the IRiSS sessions. To that end, there were internationally located individuals interested in recordings to alleviate time zone differences, such as people from the New Zealand Defense Force. Trade-offs remain. Possible options are suggested in the Next Steps section.

> *Recommendations:* If there will be future activity, collect more information on open feedback to allow deeper analysis. Increase priority for feedback surveys from the very beginning—have them pre-tested and viable by program (re)launch. Foster greater discussion mechanisms to enable InR conversations in the interim period between events. Bake into the program review plan to learn more specifics about what/how things learned are communicated back at their home organizations.

Echoing back to the first question of the event performance section—have we done well? Put another way, was the mission accomplished? Overall, yes, the IRiSS team largely completed the overarching program objectives. Moreover, the IRiSS team built a large, open, inclusive InR conversation space, recruited top minds from the InT and InR community, and people from a wide range of sectors and interests not only attended IRiSS event but engaged.

> "…I'm always on the lookout for high-quality research on insider risk, and specifically on the modeling thereof, and this is going to be immensely helpful…"
>
> – *anonymous*

A more nuanced assessment would reframe the mission accomplished question onto ARLIS' purpose to help build a capability bench to help the US government (USG) deal with emergent sociotechnical challenges and opportunities in complex systems. So, was the mission accomplished for our InR goals? Not completely, but we are working on it within our scope and other program. Looking at IRiSS' first goal:

1. Elicit and integrate diverse perspectives on InT and InR, fostering an environment that leads to better modeling (characterizing, quantifying, predicting) emergent InRs.

IRiSS was not a model building program, nor test and evaluation program. Nonetheless, the IRiSS team stepped up with an entire session dedicated to conceptualizing better models for emergent InR. The speakers, each an expert on the purpose and use of modeling at different layers of an

organization, continually circled back to thoughtful design, thinking like a modeler, and the importance of leadership. Looking at IRiSS' second goal:

2. Elicit and integrate diverse perspectives on InT and InR, fostering an environment that leads to better mitigating (shaping, exploiting, preventing) emergent InRs.

At least equally important, those same modeling speakers reinforced the important, interactive roles of context and culture help see people as part of the solution rather than the problem, a notion in of itself that already puts someone on the path toward better model building and managing the risk ecosystem. Their message interlaced with other IRiSS speakers adapting to account for social and technological changes. Intentional collaboration and diversity support better mitigation and moving the dial even further from InT to InR to Insider Trust.

> "The moment you update the [...] sessions, I'm letting my team know ASAP."
> – *anonymous*

Circling back, IRiSS was but a small piece of ARLIS' larger InR mission area; but IRiSS it made a much larger impression and appealed to a larger attendee community than initially anticipated has an outsized capability. The IRiSS impacts generated substantial buzz about the discussion space, but more importantly, it also fostered a short-term yet rich discussion on the concept, opportunity, and challenges toward an InR paradigm. However, this sort of paradigm shift does not occur overnight. So, the benefits IRiSS generated during its short six-month run will hopefully take root and grow individuals' curiosity to ask more questions about risk in complex systems and empower them to explore new ways to understand situational tolerance and apply active decision making.

ARLIS SHOWERS BRING IRiSS FLOWERS: POTENTIAL NEXT STEPS

The last section discussed IRiSS' work thus far and current position to do more. Although IRiSS ran its course, there remain opportunities to do more. Potential next steps come in three flavors: community interest, format options, and possible partnerships.

Community interest

The six-month run of IRiSS events served to whet a whistle of InR interest within the community of attendees. Culminating IRiSS in time for National Insider Threat Awareness Month (NITAM) not only provided IRiSS-goers opportunity to propagate their IRiSS conversations into other forums, but also cross-pollinate ideas back to the IRiSS team. Having already received strong, positive signals from attendee feedback for more, the conversation should be not if IRiSS will do more, but what will be done, when, and in what format.

The IRiSS work was a short-term endeavor with long-term goals. As some of our speakers pointed out, the paradigm shift will not end at InR, as we move toward Insider Trust. This is an ongoing

marathon and IRiSS' future work should be intentional about this scale, scope, and strategy. On one hand, there was community interest to do more of what we have already started. There seemed to be an appetite for series that do deeper dives, particularly on focus areas of modeling, explorations of what various private companies are doing, and how to better understand and engage with culture at the individual, team, and organizational levels. On the other hand, IRiSS can spend time doing listening sessions with our attendee base and at venues such as NITAM where new InR ideas can spread, germinate, and flourish during the post-IRiSS period. Potential areas of work here may include a larger focus on the complex, emergent systems—it is at the conceptual core of IRiSS' work, and so we have an obligation to help ensure that others fundamentally appreciate the how and why traditional analytical thinking about InT may fall short and how InR perspectives are part of the necessary sociotechnical solutions.

Format options (compare with other known / similar products)

As the seasons change and enabling new opportunities that better fit those activity spaces, so too can IRiSS evolve not only its work but its formats. The IRiSS team overcame learning curves and built and leveraged networks for the speaker series. As part of that growth period, the team encountered other activity formats that could work well for IRiSS. Some of these formats address features desired by our community, while others enable the IRiSS to branch out and take the deeper dives that might be more difficult with the current speaker series model.

Podcasts and Vodcasts

With the advent of the coronavirus pandemic and the increased use of higher quality microphones and video cameras at home, along with improvements to these technologies that are also democratized into devices like most modern smartphones, to say that podcasts and vodcasts are booming would be a massive understatement. It may seem like a saturated space, but it is also a place for individuals to discover recorded materials long into the future and offering incredible creative production flexibility.

To be clear, podcasts are an audio programs, of either a pre-determined length or open-ended series, stored online for listeners to consume on the listener's time. Vodcasts are the same as podcasts but for the addition of video, usually the video host. To avoid sounding repetitive due to their similarities, podcast here will also refer to vodcasts unless explicitly stated. Podcasts may be pre-recorded in advance, which allow for optional post-production adjustments, or they may be live-streamed where listeners can hear the cast as it is being recorded. There are also options for both, where the session can be live-streamed while it is recorded, and then later the recorded content is uploaded to the appropriate locations, again, with or without post-production.

Live streaming is a two-sided coin. On one side is the added benefit for the optional real-time engagement with listeners. Attendees can offer comments or ask questions, just as if they were sitting at any other live, in-person speaker series event. On the other hand, just like any other radio show, it is more challenging to triage live content, particularly if that content is more difficult to moderate before it is said or written. Another consideration for podcasts is where to store and

stream them; and there are a great number of podcasting sites, such ones more tailored for podcasting like Buzzsprout or Captivate, more widely known audio sites that do far more than podcasts like Spotify or Apple or Google, or multimedia sites like YouTube where it is possible to switch between Podcasting and Vodcasting.

While the tools and technologies for creating a quality podcast are becoming more readily available, there are still other costs to consider. One portion is the equipment and space—after all, this is still recorded content that should be visually and audibly pleasing, and there may be investment costs, skills to learn, and potentially the need for dedicated space to achieve high-quality, professional level content. The other portion is time. Running a live stream with immediate upload can be quick and effective; however, recorded content will almost certainly require public release review, possibly by the internal security team as well as sponsor's security review. Therefore, to keep a steady streaming schedule, which is important for any podcaster seeking to expand their base, substantial pre-planning for content should be scheduled well in advance. It may also help to have security reviewers participate in the streaming audience to provide rapid review response. There is also the production time for any quality control edits, and that time will likely be higher with vodcasting. The level of resources and planning can be far greater or just as simple as a livestream event on ZoomGov depending on the review requirements.[7]

Here are three podcasts that are at least tangentially connected to the ARLIS InR mission area's work.[8] First is Voices from the SBS Summit podcast, produced by The Threat Lab, and the National Insider Threat Task Force (NITFF). It is available on many major podcasting platforms as a monthly pre-recorded, monthly program that runs around 30 minutes with presenters from the previous year's Social and Behavioral Summit who use the podcast as an opportunity to delve deeper on their summit's presentation topic and converse with Threat Lab team members. Read more about Voices from the SBS Summit: https://castbox.fm/channel/id3991654?country=us

Insider Threat is a second podcast that follows in a similar vein to the first. Insider Threat is a biweekly production, again available on many major platforms and runs around an hour. This one is designed to be more like a radio show with multiple hosts and a featured guest speaker for a dialogue about a pre-scheduled topic. Insider Threat has a key audience community of security professionals in the State of Michigan, but its content is available widely across the Internet. Learn more about the Insider Threat podcast: https://podcast.insiderthreatpodcast.com/

The third one is the Uncovering Hidden Risks podcast. This show is a limited run series, produced by Microsoft M365 Compliance, although it is unclear when the limited run series starts and stops and currently has eight episodes available on its website, each around 30 minutes.[9] This show differs a

[7] Zoom, ZoomGov, and many other modern video conferencing platforms have various recording features already built-in for video and/or audio. Mileage may vary based on the equipment used to run it and network to stream it.
[8] Discussing these podcasts and vodcasts in no way constitutes approval of the content(s) or its creator(s).
[9] The show's website lists five episodes all uploaded on September 21, 2020, and another three episodes uploaded on May 26, 2021. It is unclear if this series is still active.

bit from the first in a few ways. First, the show embraces InR specifically in both name and content, compared to the other two that use Insider Threat as part of their branding and content, even if it includes InR content. Second, the creators have an InR blog linked to their podcast. It appears to have only one post nearly a year old, but it demonstrates a multimedia approach to engaging with the intended audience and producing materials for listeners. Learn more about Uncovering Hidden Risks podcast: https://uncoveringhiddenrisks.libsyn.com/

Other formats

Other format options include a blog, an online diary of sorts, usually open to the public, meant to express something to readers. Vlogging would be the video format of blogging and is very similar to vodcasting; nearly identical is all but purpose and more about terminology preference. Blogs are among the lowest cost options in terms of resources overall. They can be added to pre-existing websites with little-to-no additional cost and require little knowledge beyond how to operate a word processor. As such, they can be quick to produce and post, although they will likely need the public release review process like everything else. Blogs are meant to be shorter posts, rather than full length papers at several or more pages, although like most digital media, the final length is at the creator's discretion. Because blogs are stored usually as digital text, they are also popular for scraping, searching, sharing, and more. Blogs useful when you want to either get the word out about an issue or use search tools to find solutions. Unlike podcasts which often feature multiple hosts or guests, but not always, blogs are typically more individual endeavors. Shifting the number of active producers can dramatically alter the type of content put into a blog. Although yes, two people could still conduct an interview-style or other verbal engagement and then transfer it to the blog as if a transcription.

Due to the very low entry barrier costs and potential for return on attention, there are numerous companies offering their own blogs. The ease of access on the Internet also makes them a good tool for information sharing on security and other issues and a consumer and a producer, as well as a god way demonstrate expertise, and/or invite criticism to the written materials. Thus, blogs remain popular in our community, although with the popularity may also require additional security. Where podcasts may be uploaded to a major third-party company with extensive security, blogs can go on most websites with ease and the security of that blog is likely only as good as the security of that website.

Example blogs include:

- Carnegie Mellon University's Software Engineering Institute (SEI): https://insights.sei.cmu.edu/blog/topics/insider-threat/
- Code42, a cybersecurity company that actively blogs about InR and other major data and related topics: https://www.code42.com/blog/

Possible partnerships

With the IRiSS team exploring options for the future of IRiSS, including community listening, exploring conversations at other venues, and new formats, possible partnerships remain another

activity area with the potential for strong, mutual gain, but they can also come with additional responsibilities and resource consumption. The type of benefits and demands will vary greatly by the possible partner and purpose for the partnership. Additionally, one item to keep in mind that could go either way is the organizational image; partnerships could also mean being associated with that partner in good or bad ways, particularly when something goes very well or awry.

Perhaps more important than finding a potential partner is having the discussion of what IRiSS, and by extension the larger CInT / MInR team and ARLIS teams, would want and not want in a potential partner. Do they share the same vision as the IRiSS team? What is their leadership and operational culture, and are they compatible with those of the IRiSS team? Does the sector matter, whether means across the public/private divide or the types of goods or services produced? What is the organization's structure and maturity? Does that even matter depending on how much of an exchange occurs through the partnership? What might the IRiSS team be willing to provide the partner in terms of various resources, including personnel, time, and expertise?

This report does not offer any specific potential partnerships to name yet. However, there are hundreds of organizations in the IRiSS event registration and attendee records. A good place to start would be to begin with groups and individuals that have already shows a specific interest in IRiSS and its programming.

ACKNOWLEDGEMENTS

This report was prepared for [Office of the Undersecretary of Defense for Intelligence and Security (OUSD(I&S)), United States Department of Defense (DoD)] under the following agreement:

HQ003420F0655, University of Maryland, "Insider Threat and Personnel Vetting."

DISCLAIMERS

Any views, opinions, findings, conclusions, or recommendations expressed in this publication do not necessarily reflect the views of an official United States government position, policy, or decision. Additionally, neither the United States government nor any of its employees make any warranty, expressed or implied, nor assume any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, product, or process included in this publication.

Certain commercial entities, equipment, or materials may be identified in this document to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by the Applied Research Laboratory for Intelligence and Security (ARLIS), the University of Maryland, or the United States government, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

ABOUT ARLIS

Applied Research Laboratory for Intelligence and Security (ARLIS) is a UARC based at the University of Maryland College Park and established in 2018 under the auspices of the OUSD(I&S).

ARLIS is intended as a long-term strategic asset for research and development in artificial intelligence, information engineering, acquisition security, and social systems. One of only 14 designated United States Department of Defense (DoD) UARCs in the nation, ARLIS conducts both classified and unclassified research spanning from basic to applied system development and works to serve the U.S. Government as an independent and objective trusted agent.

Technical Points of Contact:

PI: Adam Russell, D.Phil.
Chief Scientist, ARLIS
301.226.8834; arussell@arlis.umd.edu

Co-PI: Kelly Jones, Ph.D.
Assistant Research Scientist, ARLIS
301.226.8850; kjones@arlis.umd.edu

Administrative Points of Contact:

Ms. Monique Anderson
Contract Officer, Office of Research Administration
Assistant Director, ARLIS
301.405.6272; manders1@umd.edu

APPENDICES

A.0: ARLIS IRiSS Team

IRiSS team

- Dr. Kelly Jones, Assistant Research Scientist and Insider Risk Mission Area Lead (Co-PI)
- Joseph Kelly, Director of Computational and Information Technology and Professor of the Practice
- William (Bill) Stephens, Director of Counterintelligence Research, and Professor of the Practice
- Dr. Adam Russell, Chief Scientist and Insider Risk Mission Area Lead (PI)
- Shawn Janzen, Graduate Research Fellow and IRiSS Coordinator

Bios

Dr. Kelly Jones is an experimental and social psychologist at the Applied Research Laboratory for Intelligence and Security, a University-Affiliated Research Center of the United States Department of Defense supporting the Intelligence Community. She currently serves as the Co-PI of the Insider Risk Research Program, leading a diverse portfolio of projects in social/behavioral science research and test, evaluation, verification, and validation (TEV&V) work for both InT and personnel vetting applications, in addition to her work in the Cognitive Security mission area on cutting edge research methods. Before being appointed an assistant research scientist, she was a postdoctoral researcher at ARLIS, where she was the science and technical lead on InT research initiatives. Prior to ARLIS, Jones was an Assistant Professor of Psychology at Limestone College, where she founded and served as the director of the Social Attitudes, Behaviors, and Cognitions Research Lab (Social ABCs Lab), leading research projects in a variety of individual and social perceptions and behaviors, including cognitive biases and attitudes and behaviors regarding cultural and social movements. Dr. Jones holds a PhD in Experimental Psychology from the University of North Dakota, a MA in Experimental Psychology from the University of North Dakota, and a BA in Psychology from Messiah College.

Joseph Kelly is a versatile business leader and strategist with 30 years of experience educating senior leaders in the public and private sectors on intelligence, risk, and their intersection with information and communications technologies. He is a recognized expert on the intersection of technology, policy and strategy – with deep expertise in the changing cybersecurity landscape.

During his 20 years in government as both a federal employee and a contractor, he advised executive leaders in government and industry on the strategic implications

of emerging technology, cyberspace operations, global influence, and international governance regimes. He served as the Acting CIO and Senior Technical Advisor for the US Government's Privacy and Civil Liberties Oversight Board, focused on how emerging technologies challenge current assumptions about policy, law, and economics. Within the Department of Defense (DoD), he served as Deputy Director for Cyber Capabilities, Chief of Cyber Intelligence, and as the Head of the Information Operations (IO) Policy and Plans in the Office of the Under Secretary of Defense for Intelligence. At DoD, he was intimately involved with the establishment of US Cyber Command, the development of DoD and national policies on cyberspace, coordination of cyberspace policy and research with allies, and assessment of the threats posed by foreign investment in technology. As President of Pointweaver, LLC, Mr. Kelly works as a consultant advising multi-billion dollar commercial clients on cybersecurity, operational and geopolitical business risk, and government foreign investment reviews and mitigation plans. Over the span of about two decades, Mr. Kelly provided support to DoD, the National Intelligence Council, the Navy, the Air Force, and the Army on the future of technology evolution. He holds an MA in International Relations and Economics from Johns Hopkins School of Advanced International Studies (SAIS) and a BA in Government from Georgetown University.

William Stephens is a Professor of Practice and Director of Counterintelligence Research at ARLIS who recently arrived after serving 11 years in the Defense Intelligence Senior Executive Service at the Defense Counterintelligence and Security Agency (DCSA) as the Assistant Director for Counterintelligence; and prior to that position, he served 27 years as a USAF Officer in the Air Force Office of Special Investigations, primarily in the field of counterintelligence.

Mr. Stephens has enjoyed an extensive career of success in leading intelligence, counterintelligence (CI), security, and InT teams--small, medium, and large--to defend U.S. and Allied government and private sector interests in permissive, non-permissive, and coalition environments in Europe, South Asia, East Asia, and U.S. Mr. Stephens conceived, designed, and implemented counter industrial espionage and counterintelligence operations globally in defense of the private sector and industrial base. He pioneered the pan-governmental "Deliver Un-compromised" initiative and employed commercial due diligence techniques, including supply chain risk and InT efforts to deter, detect, and disrupt adversaries penetrating and exploiting U.S. and Allied industrial bases. During his government career, Mr. Stephens built deep practical expertise in counterintelligence, security, national security policy, and regulation for defense industrial base security, Foreign Ownership, Control, or Influence.

His education includes BS, Business Administration, Auburn University; MS, Management, Central Michigan University; MS, National Security Studies (East Asia—Philippines), US Naval Postgraduate School; MS, Strategic Resourcing, National Defense University. Notable training includes: DoD General Officer Course (CAPSTONE), National Defense University; DoD SES Course (APEX), National Defense University; Senior Managers in Government, Harvard Kennedy School of Government.

Dr. Adam Russell is Chief Scientist at UMD's Applied Research Laboratory for Intelligence and Security (ARLIS), with an adjunct faculty position in UMD's Department of Psychology. Adam began his career in national security working on human performance and strategic competitions for various government organizations. After joining the government in 2009, he spent the next decade as a Program Manager at the Intelligence Advanced Research Projects Activity (IARPA) and then the Defense Advanced Research Projects Agency (DARPA) - where he was known as the "DARPAnthropologist." At IARPA and DARPA, Adam managed a large portfolio of high-risk, high-impact R&D programs focused on enhancing the USG's Human Domain capabilities to better understand, anticipate, and leverage human social behavior and variability through improving scientific discovery, innovation, and reproducibility, especially in the social and behavioral sciences (e.g., Next Generation Social Science (NGS2), Collective Allostatic Load, Systematizing Confidence in Open Research and Evidence (SCORE), Ground Truth, How the Social Becomes the Biological, Strengthening Human Adaptive Reasoning and Problem-solving (SHARP), Tools for Recognizing Useful Signals of Trustworthiness (TRUST), and ODNI and IARPA's first public data analysis incentive "Challenge" competition, INSTINCT).

Adam has a BA in cultural anthropology from Duke University and a D.Phil. in social anthropology from Oxford University, where he was a Rhodes Scholar. He has played rugby for Oxford University - representing Oxford in four Varsity matches - as well as the US Men's National Rugby Team, and was the High-Performance Director for the US Women's National Rugby Team for the 2014 and 2017 Rugby World Cups. He currently serves as the Head Sport Scientist for the Athlete Collective.

Shawn Janzen is a Graduate Research Assistant at ARLIS and a Ph.D. Candidate and lecturer in the UMD College of Information Studies. His research interests include how individuals and organizations create, choose to share, and adopt information that becomes part of the institutional knowledge, engagement, and administration. He focuses these interests on issues related to disruptive and emerging technologies, cybersecurity, ethics, networks, and public policy. Professionally, Shawn consulted for clients on organizational communications and digital strategy, transportation policy and government contracting, and data ethics.

Shawn served in the U.S. Peace Corps in St. Vincent and the Grenadines as an NGO and institution developer. He was a researcher at the European Parliament, the Chicago Council on Global Affairs, and George Mason University. His nonprofit management work spans more than a decade, with service work advising several boards including ASPA chapters in DC and Chicago as well as the United Nations Association-USA Greater Chicago Chapter. Shawn enjoys teaching methods courses

and serving as a conduit for student success. He was twice awarded the Student's Choice Teaching Award in 2018 and 2019.

A.1: SPEAKER BIOS

A.1.1: Event #1 Speaker bios

Event: State of Insider Threat and Insider Risk paradigms

Guest speakers

- Doug Thomas, Counterintelligence Operations and Investigations, *Lockheed Martin Corporation*
- Matt Eanes, Director of the interagency Performance Accountability Council, *Program Management Office (PAC PMO)*
- Dr. Natalie Scala, Associate Professor, *Towson University*
- [Name redacted], *[Title redacted – High level manager that leads insider risk]*, *[Company name redacted — large, private media communications company]*

Bios

Doug Thomas
Director, Counterintelligence Operations and Investigations, *Lockheed Martin Corporation*

Douglas D. (Doug) Thomas is the Director, Counterintelligence Operations and Investigations for Lockheed Martin Corporation. In this capacity, he leads a staff that is responsible for providing advice and guidance relative to investigations, counterintelligence, counterterrorism, and workplace violence matters impacting the Corporation. He is also the primary face to the Intelligence Community. Prior to joining Lockheed Martin, Mr. Thomas was the Principal Deputy Director of Counterintelligence under the Office of the Director of National Intelligence and chaired the National Counterintelligence Operations Board, which informed the President on the gravest intelligence threats facing the United States, and the National Counterintelligence Strategy, which informed the President of how the Intelligence Community would mitigate those threats. Mr. Thomas also served as a Special Agent for 25 years with the Air Force Office of Special Investigation and is a retired member of the Senior Executive Service. Mr. Thomas holds a bachelor's degree in Asian Studies.

Matt Eanes
Director of the interagency Performance Accountability Council, *Program Management Office (PAC PMO)*

Matt Eanes serves as the Director of the interagency Performance Accountability Council's Program Management Office (PAC PMO). The office helps coordinate personnel vetting reform across the Executive Branch. Matt assists the PAC's leadership with implementing its Trusted Workforce 2.0 initiative, a series of reforms that will dramatically modernize the Federal Government's personnel vetting mission space. Prior to joining the PAC PMO, Matt worked as a consultant on range of government and private sector issues. He earned a master's degree in systems engineering from Virginia Tech.

Dr. Natalie Scala
Associate Professor, *Towson University*

Dr. Scala is a tenured associate professor and director of the graduate programs in supply chain in the College of Business and Economics at Towson University. Her research specializes in decision analysis, with applications in cybersecurity, defense, and spare parts. Her main focus right now is cyber, physical, and InTs to voting processes, especially at polling places. This includes a model InT risk management as well as training for pollworkers. Dr. Scala provides consulting services as an analyst with Innovative Decisions, Inc., and has extensive experience working with government clients and in the electric utility industry. Dr. Scala earned a Ph.D. in industrial engineering from the University of Pittsburgh.

[Name redacted]
High level manager that leads insider risk at a large, private media communications company

[Bio redacted]

A.1.2: Event #2 Speaker bios

Event: From threat to risk: Gain & loss, response, and management around insiders within academic environments

Guest speakers

- Dr. Kevin Gamache, CSRO, *The Texas A&M University System*

- Dr. Lauri Locascio, VP for Research, *UMD College Park & UMD Baltimore*

Bios

Dr. Kevin Gamache
Chief Research Security Officer, *The Texas A&M University System*

Dr. Kevin Gamache is responsible for ensuring A&M System member universities are compliant with U.S. Government requirements for protecting sensitive federal information. He is also on the faculty of the George Bush School of Government and Public Service at Texas A&M University in College Station. He established and leads the Academic Security & Counter Exploitation Program, an association of U.S. universities established to help heighten security awareness in academia. He received a Doctor of Philosophy degree from Texas A&M University and a Master of Science Degree from the Industrial College of the Armed Forces.

Dr. Laurie Locascio
Vice President for Research, *the University of Maryland, College Park and the University of Maryland, Baltimore*

Dr. Locascio oversees the University of Maryland's vibrant research and innovation enterprise at these two campuses, which garner a combined $1.1 billion in external research funding each year. Within Locascio's purview are the development of large interdisciplinary research programs, technology commercialization, innovation and economic development efforts, and strategic partnerships with industry, federal, academic, and nonprofit collaborators. She is a professor in Maryland's Fischell Department of Bioengineering, and professor (secondary) in the Department of Pharmacology at the University of Maryland School of Medicine. Dr. Locascio previously worked at the National Institute of Standards and Technology (NIST), most recently as Acting Principal Deputy Director and Associate Director responsible for leading the internal scientific research and laboratory programs across two campuses in Gaithersburg, MD and Boulder, CO. Locascio received a B.Sc. in chemistry from James Madison University, a M.Sc. in bioengineering from the University of Utah, and a Ph.D. in toxicology from the University of Maryland, Baltimore. As a biomedical researcher, she published more than 100 scientific papers and 12 patents.

A.1.3: Event #3 Speaker bios

Event: Industry views – Where are we now

Guest speakers

- Stephen Szypulski, Vice President, Global Compliance Division, *Goldman Sachs*
- Caroline Gilman, Program Manager, Insider Risk Management Program, *Booz Allen Hamilton*

- Dr. David Mussington, Executive Assistant Director, Infrastructure Security Division, *CISA*

Bios

Stephen Szypulski
Vice President, Global Compliance Division, *Goldman Sachs*

The Conduct & Integrity Team is principally responsible for the firm's global Compliance Conduct Program, Business Integrity Program, and Firmwide Insider Threat Program, and helps mitigate the risk of employee misconduct globally. Stephen joined Goldman Sachs in 2015 and previously was a member of Financial Crime Compliance's (FCC) Financial Intelligence Unit (FIU) and Forensics teams. He was named associate in 2017 and vice president in 2019. At Goldman Sachs, Stephen is a member of the Firmwide LGBT Network. Prior to joining the firm, Stephen served as Aide to Mayor Steven Fulop in Jersey City, New Jersey, where he served as the mayor's traveling aide in New Jersey's second largest city. Stephen earned a bachelor's degree from Georgetown University's School of Foreign Service and a master's degree from Columbia University. He served as Fulbright Scholar in Poland from 2012-2013, and is currently based in New York.

Caroline Gilman
Program Manager, Insider Risk Management Program, *Booz Allen Hamilton*

Caroline Gilman manages Booz Allen's Insider Risk Management Program (IRMP). Caroline leads a team that identifies, analyzes, and mitigates risks to Booz Allen's trusted employees, intellectual capital and critical business operations, client sensitive data entrusted to firm employees, and Booz Allen's reputation as a leader in strategy and technology consulting. Prior to leading the IRMP, Caroline worked as an IT Project Manager, gaining a unique perspective into IT system requirements, capabilities and integrations. Caroline is a certified Project Management Professional and CERT Insider Threat Program Manager Certificate Holder.

Dr. David Mussington
Executive Assistant Director, *Infrastructure Security Division, Cybersecurity and Infrastructure Security Agency (CISA)*

As Executive Assistant Director, Dr. Mussington helps lead CISA's efforts to secure the nation's critical infrastructure in coordination with government and the private sector. Key areas of focus include vulnerability and risk assessments; securing soft targets and crowded places; training and exercises; and securing high-risk chemical facilities. Prior to joining CISA, Dr. Mussington was Professor of the Practice and Director for the Center for Public Policy and Private Enterprise at the

School of Public Policy for the University of Maryland. His research and teaching activities focused on cyber-physical system risk management, election cybersecurity, and critical infrastructure security risk management. Dr. Mussington has extensive private and public sector experience on counter terrorism, cyber security studies, and cyber risk assessments. Click here for a longer biography. Dr. Mussington has a Doctorate in Political Science from Canada's Carleton University. He also received a Bachelor of Arts and a Master of Arts degree in Economics and Political Science from the University of Toronto.

A.1.4: Event #4 Speaker bios

Event: Tools, methods, and technology -- State of the art in modeling
Guest speakers

- Jeffrey (J.C.) Dodson, Chief Security Officer, *BAE Systems Inc.*
- Katherine Hibbs Pherson, Chief Executive Officer, *Pherson Associates*
- Andrew Moore, Lead Insider Threat Researcher & Senior member of the technical staff, CERT Division, *Software Engineering Institute (SEI)*

Bios

Jeffrey (J.C.) Dodson
Chief Security Officer, *BAE Systems Inc.*

Mr. Dodson is responsible for corporate security strategy, operations and assurance. His risk management portfolio includes all elements of industrial, international and cyber security for U.S. and overseas operations. Prior to his CSO appointment in 2020, Mr. Dodson was BAE's Global Chief Information Security Officer (CISO). He has served in a variety of executive positions with program management, strategy, business development and security. He joined BAE Systems in 2002 following a 22-year career with the U.S. Air Force that included flying operations, weapons system acquisition management, and command assignments. Mr. Dodson currently serves on the Board of Directors for the National Defense-Information Sharing and Analysis Center (ND-ISAC). He is a member of the Department of Homeland Security's Defense Industrial Base Sector Coordinating Council and an industry contributor/advisor to numerous U.S. Government national security policy studies and initiatives.

Katherine Hibbs Pherson
Chief Executive Officer, *Pherson Associates*

Ms. Pherson teaches advanced analytic techniques and critical thinking skills to analysts in the Intelligence Community, homeland security community, and the private sector. She is a consultant to the government on planning, security, communications, and analysis projects. She and

Randy Pherson are co-authors of Critical Thinking for Strategic Intelligence, 3rd ed. (Sage/CQ Press, 2020). Ms. Pherson also serves as President of Globalytica, LLC, the commercial, and international arm of Pherson Associates. She is vice chair of the Intelligence and National Security Association's (INSA) Security Policy Reform Council and a Trustee of the Intelligence and National Security Foundation. She also is chair of the Industrial Security Working Group's (ISWG) Department of Homeland Security (DHS) Focus Group and a member of AFCEA International's Intelligence Committee and ASIS International's Defense and Intelligence Council. Ms. Pherson in 2000 completed a 27-year career with the Central Intelligence Agency in intelligence and security analysis and resource management. Her leadership in the security arena led to the adoption of a risk management methodology, the strengthening and the implementation of overseas security countermeasures, and improvements in dealing with unsolicited contacts. As Director of the Director of Central Intelligence's (DCI) Center for Security Evaluation she managed the Intelligence Community's involvement in rebuilding the penetrated US Embassy in Moscow. Ms. Pherson received her A.B. in Hispanic Studies from Vassar College, an M.A. in Spanish Linguistics and Latin American Studies from the University of Illinois, and an M.A. in Communications from the University of Oklahoma. She is a recipient of the CIA's Distinguished Career Intelligence Medal and the Intelligence Community's National Distinguished Service Medal.

Andrew Moore
Lead Insider Threat Researcher & Senior member of the technical staff, CERT Division, *Software Engineering Institute (SEI)*

Mr. Moore works with teams across the SEI applying modeling and simulation techniques to cybersecurity and to system and software engineering problems. He has over 30 years of experience developing and applying mission-critical system analysis methods and tools, leading to the transfer of critical technology to both industry and the government. His research interests include socio-technical system simulation modeling and analysis, cybersecurity, InT, software acquisition and sustainment, IT controls analysis, survivable systems engineering, and system risk analysis. Before joining the SEI in 2000, Mr. Moore worked for the U.S. Naval Research Laboratory (NRL) developing, analyzing, and applying high-assurance system development methods for the Navy. He has served as principal investigator on numerous projects sponsored by ODNI, OSD, NSA, DARPA, and CMU's CyLab. Mr. Moore has published a book, two book chapters, a special journal issue on InT modeling and simulation, and a wide variety of technical journal and conference papers. Mr. Moore holds a BA in Mathematics and Computer Science from The College of Wooster, an MA in Computer Science from Duke University, and a graduate certificate in System Dynamics Modeling and Simulation from Worcester Polytechnic Institute.

A.1.5: Event #5 Speaker bios

Event: Insider risk, human resources, and the human capital supply chain challenge

Guest speakers:

- Charles Phalen, Principal, *CS Phalen & Associates LLC*; former Acting Director, DCSA; former VP Corporate Security, *Northrup Grumman*
- Heather McMahon, Lieutenant Colonel (ret.), *US Army*; Professor of Practice, *ARLIS*; former Senior Director, *President's Intelligence Advisory Board*
- [Name redacted], *[Title redacted – Corporate officer for insider risk and counterintelligence]*, *[Company name redacted — Major private consulting firm]*

Bios

Charles Phalen
Principal, *CS Phalen & Associates LLC*
former Acting Director, *DCSA*
former VP Corporate Security, *Northrup Grumman*

Charles S. Phalen is currently the principal and independent consultant at C S Phalen & Associates, LLC. He is an accomplished senior security executive with over four decades of experience including over sixteen years leading security programs at four federal agencies and a major defense company during periods of unprecedented growth, development, and challenge. Key areas of experience include the full range of security operations, national and international crises, government and industry partnerships, continuity of operations, business process reengineering, organizational development, P&L, and mergers. Mr. Phalen served as the Acting Director of the Defense Counterintelligence and Security Agency (DCSA) from June 2019 through March 2020. Mr. Phalen and his leadership team successfully merged the Office of Personnel Management's background investigation program with DOD's Defense Security Service. The merged agency includes approximately 12,000 federal and contract personnel executing the government-wide personnel vetting program and the critical technology protection mission. Mr. Phalen was the Director of the National Background Investigations Bureau, an organizational element of the U.S. Office of Personnel Management, from October 1, 2016 to September 30, 2019 (overlapping from June through September 2019 with the Acting Director/DCSA assignment). In this role, he led a government-wide organization providing investigations for national security, suitability, and credentialing determinations for more than 100 federal agencies. In his previous position, Mr. Phalen was Vice President of Corporate Security for Northrop Grumman Corporation and led the global security organization responsible for overseeing the security policies, procedures and processes that protect company employees, information, assets, and property worldwide. Prior to that, Mr. Phalen spent 30 years in the federal service. His most recent government positions include Director of Security for the Central Intelligence Agency; Assistant Director, Security Division, Federal Bureau of Investigation; Chief, Protective Programs Group, CIA Office of Security; Executive Officer, CIA Office of Security; Center Chief, CIA Office of Facilities and Security Services; and Chief, Facilities and Information Security Division, National Reconnaissance Office. Previously, he worked in managed security activities involving investigations, operations support, risk analysis, and facility and asset protection, in the United States and abroad. Mr. Phalen has a bachelor's degree in law enforcement and criminology from the University of Maryland. He is active in a number of external security organizations and forums.

Heather McMahon
Lieutenant Colonel (ret.), *US Army*
Professor of Practice, *ARLIS*
former Senior Director at *President's Intelligence Advisory Board*

Heather is a former DoD intelligence senior executive and seasoned combat veteran currently serving as a Professor of Practice at the Applied Research Laboratory for Intelligence and Security and as a consultant where she advises on national security, counterintelligence, human intelligence, InT, critical technology protection, supply chain risk management and industrial security concerns. A highly skilled human intelligence and counterintelligence officer with deep operational experience honed through close to three decades of world-wide service, Heather's experience is particularly relevant today as companies struggle to balance risk and reward while defending themselves from the onslaught of threats from state-sponsored IP theft, cyberattacks and malicious insiders. A West Point Graduate, she served extensively abroad in Afghanistan, Iraq, Bosnia, Europe, and Asia while serving US Army at every echelon between platoon and corps, as well as in the intelligence community's strategic enterprise, Heather transitioned to the technology sector before returning to serve the nation as a senior executive, where she served at the White House's President's Intelligence Advisory Board, the Undersecretary of Defense for Intelligence, and the Army Staff. Heather earned a Bachelor of Science from West Point and is a graduate of numerous advanced intelligence community and military schools, to include Jumpmaster and Airborne School. She is an Advisory Board member at the Gula Tech Foundation, a civic effort focused on closing the cyber skills gap in America. She is also national security fellow at the Foundation for Defense of Democracies and serves as volunteer Senior Advisor the Maker Mask, a nonprofit technology-based effort to support effective community responses to the COVID-19 crisis.

[Name redacted]
[Title redacted – Corporate officer for insider risk and counterintelligence],
[Company name redacted — Major private consulting firm]

[Bio redacted]

A.1.6: Event #6 Speaker bios

Event: Actualizing the Insider Risk paradigm

Guest Speakers

- [Name redacted], [Title redacted – High level office leader], *[Company name redacted — US government defense intelligence related agency]*
- Robert (Bob) Rohrer, Assistant Director for Insider Threat, *National Counterintelligence and Security Center (NCSC)* and Director, *National Insider Threat Task Force (NITFF)*
- MaryJo (MJ) Thomas, Director of Security, *General Dynamics Bath Iron Works*
- LTG (ret.) Darsie Rogers, Professor of Practice, *ARLIS* and General (ret.), *U.S. Army & Defense Threat Reduction Agency*

Bios

[Name redacted][10]
[Title redacted – High level office leader], *[Company name redacted — US government defense intelligence related agency]*

[Bio redacted]

a senior advisor to the Secretary of Defense and the Under Secretary for Intelligence & Security. Prior to her role as the Deputy, Ms. Jones served as the Chief of Staff to the Director for Defense Intelligence. Ms. Jones previously served in the Office of the Under Secretary of Defense for Policy, where she led policy development and implementation for the Deputy Assistant Secretary of Defense for Stability and Humanitarian Affairs in the Office of the Assistant Secretary of Defense for Special Operations and Low Intensity Conflict. In this position, she was responsible for a broad range of issues related to International Humanitarian Law, Human Rights, and international engagement. She was the Department's liaison to the International Committee of the Red Cross, and Policy's focal point for international treaty implementation and reporting.

Ms. Jones was previously assigned to the Office of Rule of Law and Detainee Policy, where she led policy implementation and strategic communication efforts to ensure the Department's detention policy was principled, credible, and sustainable for 21st century warfare. Prior to her Policy positions, Ms. Jones served in the Department's Public Affairs office, where she planned and executed special events and outreach activities for the Secretary of Defense, including to analysts, think tanks, and other interested parties. Prior to her career at DoD, Ms. Jones was a legislative aide to a United States Senator, working primarily on defense and foreign policy issues. Ms. Jones has a Bachelor's degree in Journalism from the University of Nevada (Reno) and a Master's degree in National Security and Strategic Studies from the Naval War College.

[10] [Name redacted] was a welcomed alternate speaker for Mr. Garry Reid, the Director for Defense Intelligence, who was originally scheduled but unable to attend at the last minute due to matters of national security.

Robert Rohrer
Assistant Director for Insider Threat, *National Counterintelligence and Security Center (NCSC)*
Director, *National Insider Threat Task Force*

Robert "Bob" Rohrer currently serves as the National Counterintelligence and Security Center (NCSC) Assistant Director for Insider Threat and as the Director of the National Insider Threat Task Force (NITFF). Housed within NITFF is an interagency task force co-chaired by the Office of the Director of National Intelligence (ODNI) and the Department of Justice. Mr. Rohrer is a long-time member of the NCSC leadership team, having joined the NCSC in 2015 after a decade in the Intelligence Community, supporting global counterterrorism and counterintelligence activities. Most recently, he served as the Deputy Assistance Director for the NCSC Mission Integration Directorate overseeing a wide spectrum of national level programs. Previously, Mr. Rohrer served at the Deputy Director of the NITFF from 2017 to 2020 and the Technical Director the year prior. Mr. Rohrer brings a broad spectrum of experience in criminal and national security investigations, intelligence, counterintelligence, physical and electronic surveillance, and counterintelligence operations. He began his career in 1992 as a Special Agent with the U.S. Immigration and Naturalization Service (INS) in Los Angeles, investigating human smuggling/trafficking, document/benefit fraud, and other Federal crimes. Mr. Rohrer led the creation of the INS's first field-level Technical Surveillance Unit, and supported undercover and wiretap operations throughout the Southwestern United States. In 2000, he became a Supervisory Special Agent, leading the Los Angeles INS Benefit Fraud and Technical Operations Units. In 2002, Mr. Rohrer became Section Chief (INS equivalent of an Assistant Special Agent-in-Charge) in San Diego, and in 2003, with the creation of the Department of Homeland Security (DHS), he came to Washington, D.C. as part of the U.S. Immigration and Customs Enforcement (ICE) transition team, merging legacy customs and immigration investigation programs into one organization. At ICE Headquarters, Mr. Rohrer served as the Chief of the ICE Compliance Enforcement Unit, and the Senior ICVE Liaison to the Central Intelligence Community. Mr. Rohrer holds a Bachelor of Science in Criminal Justice from California State University at Long Beach, and a Master of Science in Technology Management / Homeland Security Management from the University of Maryland, University College.

MJ Thomas
Director of Security, *General Dynamics Bath Iron Works*

MaryJo “MJ” Thomas is Director of Security at General Dynamics Bath Iron Works. She is responsible for overseeing all BIW Security functions including cyber, industrial and physical plant security programs. She manages day-to-day activities and ensures compliance with all programmatic, regulatory, legal and contractual requirements for these areas. She has extensive experience in matters concerning national security and the protection of defense weapons and technology, with specific expertise in crisis and change management and

investigative leadership. Ms. Thomas spent much of her professional career with the Federal Bureau of Investigation. Her most recent assignment was as FBI Senior Advisor to the Department of Defense for the FBI National Security branch. She was the primary interface between the FBI and the Office of Secretary Defense on national security issues which involved the FBI and she coordinated counterintelligence, counterterrorism, cyber and weapons of mass destruction matters between the two agencies. Her previous roles include Section Chief of the Counterproliferation Center in the FBI's Counterintelligence Division. Ms. Thomas joined the FBI as a special agent in 2000 after serving as a law enforcement officer in Rhode Island. Ms. Thomas also has served as a Security Forces Officer and Logistician in the Air Force, active duty and reserve. She earned a bachelor's degree from Providence College, graduated from the Rhode Island Municipal Police Training Academy and the Academy of Military Science.

LTG (ret.) Darsie Rogers
Professor of Practice, *ARLIS*
General (ret.), *U.S. Army & Defense Threat Reduction Agency*

LTG(R) Darsie D. Rogers, Jr. served in our Nation's Army for over 34 years leading adaptable and high-performing teams in solving challenging problems in uncertain environments. As a Special Forces Soldier, Darsie served in the Pentagon and around the world, rising to the rank of three-star general. Darsie's military service saw combat through the dynamic and ambiguous environments of the Gulf War, Iraqi Freedom/New Dawn and numerous contingency operations. Later he was responsible for leading US Special Operations Forces in the Middle East where he routinely engaged with US Ambassadors, Government Agencies, regional partner nations, and senior foreign government dignitaries and officials to protect US national interests. He culminated his career at the Defense Threat Reduction Agency tasked with countering weapons of mass destruction and improvised threats. Darsie retired from active duty and joined the University of Maryland in August of 2020. He serves on the board of several non-profit and charitable entities and advises private-sector organizations. He earned a Bachelor of Arts from Auburn University, a Master of Arts from Louisiana State University, and a Master of Science in Strategic Studies from the US Air Force War College.

A.2: EVENT ANALYTICS

This appendix showcases some of the post-event summary statistics for individual event tracking, types of organizations, and recaps feedback poll results from the fifth and sixth events. Data for this analysis came from the registration and attendance logs generated by ZoomGov. For the purposes of event analysis, most tracking was done through a combination of email address and name inspection for those who appeared in one or both event logs for each event.

Attendance Reporting

Table 5 displays each of the six IRiSS events, along with the total number of people who registered and attended each event. Matching exact attendance is somewhat problematized because individuals may have called into the ZoomGov session which may not link back to their registered login details, such as using one of the standard call-in phone numbers that only requires the meeting ID. Therefore, Table 5 presents two attendance options. The *without* phone value is a low range estimate which could occur if all the phone numbers that called in were also represented by someone already logged into their ZoomGov application. The *with* phone value is the flipside position, whereby no caller was also simultaneously logged into the ZoomGov applications.

Table 5: Participation Overview

Event	RSVP	Attend (w/o phone)	% Attend (w/o phone)	Attend (+ phone)	% Attend (+ phone)
#1 Kickoff	468	221	47%	246	53%
#2 Academia	380	195	51%	231	61%
#3 Industry	281	165	59%	183	65%
#4 Modeling	407	183	45%	207	51%
#5 Workforce	315	176	56%	194	62%
#6 Capstone	338	171	51%	202	60%

Event registration fluctuated from a low of 281individuals (Industry) to 468 (Kickoff). Despite this range, attendance turnover averaged 51% without phones and 58% with phones. Hovering above the 50% benchmark put IRiSS slightly ahead of the expected turnover rate.[11] Free-to-attend events, like IRiSS, tended to suffer more on turnover due to the no-loss impact for not joining a registered session, unlike if someone buys an event ticket—not using that event ticket then incurred a loss value equal to the ticket cost. Interestingly, the Kickoff event may have had the highest registration because of the newness of the IRiSS program but had some of the lower attendance turnovers. Conversely, the Industry event with the lowest registration had the highest attendance turnover. From the rather steady attendance, it could be that this consistency comes from IRiSS developing a regular attendee base.

Optionally provided organization data helped assign the individual as belonging to a type of organization: government, academic, private / nonprofit organizations, or unknown; a phone classifier was as subclass of unknown but made into its own category due the large quantity of phone numbers. Organization assignment used manual classification through visual inspection of email address domains and the provided organization names.[12] Table 6 showcases the results of this

[11] Rappaport, Rachel. (2020, December 18). 10 Virtual Event Benchmarks to Know for 2021. Bizzabo. https://blog.bizzabo.com/virtual-event-benchmarks

[12] Classification errors may exist through unfamiliar organization names or when a group mismatch existed between email address and known organization type, such as a university email but a government agency organization name. This may occur when a person has multiple affiliations and the group code only allowed for a single classification.

classification. While the IRiSS team expected most of the engagement to come from the USG and second from private companies, it was a bit surprising to see these values reversed. A closer look at the specific companies involved may be needed to distinguish this further.

Table 6: Attendee Organization Affiliation by Group

Group	# Attendees	% Attendees
Government	437	34%
Private / NPO	553	43%
Academia	163	13%
Phone	130	10%
Unknown	17	1%
Total	1300	100%

Tables 7 and 8 take a deeper dive to assess the rates at which individuals came back for additional IRiSS events. Table 7 shows the data as frequency counts and Table 8 has the data results as percentages with row totals. From here, the first key data point is that the IRiSS events caught the attention of 1,300 unique individuals across all six events; this number is most likely a bit smaller since 130 (10%) of those entries were unique phone numbers. Across these two tables in general, zero rightly indicates there were no individuals registering or attending that number of events. However, the zero columns in both Tables 7 and 8 can be a bit deceiving. For attendance, values in the zero column reflect those who did not attend an event; yet there are some individuals who also did not register for any events. A safe assumption would be that a person must register to attend; however, this did not appear to be the case for at 143 people. This is a non-trivial number, and the IRiSS Coordinator is still exploring how that may occur. One speculation posited it could be due to individuals who obtained the dial-in number and meeting ID without first registering. Another included discrepancies in how ZoomGov recorded attendance in a regular event session compared to the more traditional webinar session; the forms generated have slightly different tracked data.

While raw counts in Table 7 have their uses, the percentages of Table 8 may help ease into discussion points. Of the 1,300 individuals interested in an IRiSS event, approximately half of them registered for only one event and about 42% attended one event. From here, there was a step decline in engagement with the entire series. About one-fifth of the individuals registered for two events, and only about half of those (11%) attended two events. The remaining number of event registration and attendance collapsed into the single digit percentages. This suggested most people interested in IRiSS might have been interested in just one of our topical event sessions, such as the modeling or workforce sessions. It is also possible that a person attended one event and found it not to their liking, and which point they decided not to return for more. Anecdotally, the latter might not be the case, since the IRiSS Coordinator sent out email updates for initial registration and follow-up reminders to people who previously signed up; with the ever-increasing list of people that is nearly 1,300, only a handful of perhaps three people requested to be removed from the email outreach as a sign of disinterest. The two feedback pools offered some insight here, but ultimately, hard data asked to these individuals is necessary to explore this speculation any further. A positive finding from these tables was that even though the percentages were relatively small for engaging with three or more events, the frequency counts still signaled having a sizable crowd—261 people registered, and 110 people attended three or more events. Crowds this large would normally require large meeting spaces, making the virtual environment ideal.

Table 7: Individual Return (#)

Frequency	Events	0	1	2	3	4	5	6	Total
	RSVP	143	643	253	114	77	53	17	1300
	Government	1	261	92	38	23	16	6	437
	(Non)Profit	6	291	118	61	43	28	6	553
	Academia	1	85	41	12	10	9	5	163
	Phone	130	0	0	0	0	0	0	130
	Unknown	5	6	2	3	1	0	0	17
	Attend	488	554	148	66	25	13	6	1300
	Government	229	147	40	14	5	2	0	437
	(Non)Profit	205	215	66	39	19	8	1	553
	Academia	48	74	24	8	1	3	5	163
	Phone	0	111	16	3	0	0	0	130
	Unknown	6	7	2	2	0	0	0	17

Note: Event count 0 is an indicator for those that phoned into the event or were able to attend without first registering an email address.

Table 8: Individual Return (%)

Percentages	Events	0	1	2	3	4	5	6	Total
	RSVP	11.0%	49.5%	19.5%	8.8%	5.9%	4.1%	1.3%	100%
	Government	0.2%	59.7%	21.1%	8.7%	5.3%	3.7%	1.4%	100%
	(Non)Profit	1.1%	52.6%	21.3%	11.0%	7.8%	5.1%	1.1%	100%
	Academia	0.6%	52.1%	25.2%	7.4%	6.1%	5.5%	3.1%	100%
	Phone	100.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	100%
	Unknown	29.4%	35.3%	11.8%	17.6%	5.9%	0.0%	0.0%	100%
	Attend	37.5%	42.6%	11.4%	5.1%	1.9%	1.0%	0.5%	100%
	Government	52.4%	33.6%	9.2%	3.2%	1.1%	0.5%	0.0%	100%
	(Non)Profit	37.1%	38.9%	11.9%	7.1%	3.4%	1.4%	0.2%	100%
	Academia	29.4%	45.4%	14.7%	4.9%	0.6%	1.8%	3.1%	100%
	Phone	0.0%	85.4%	12.3%	2.3%	0.0%	0.0%	0.0%	100%
	Unknown	35.3%	41.2%	11.8%	11.8%	0.0%	0.0%	0.0%	100%

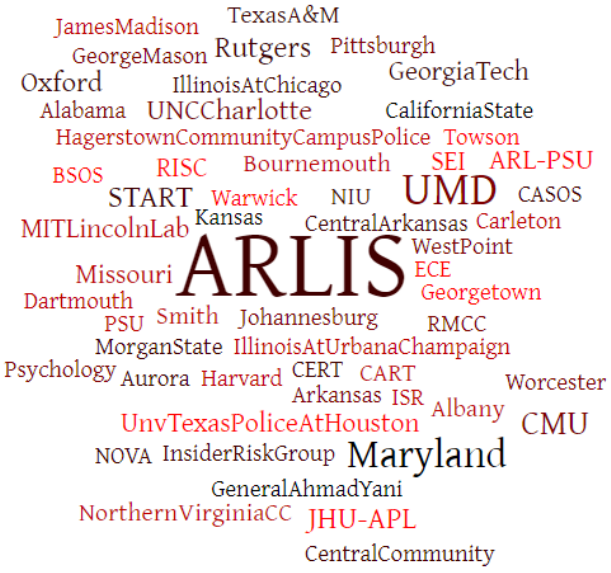
Note: Event count 0 is an indicator for those that phoned into the event or were able to attend without first registering an email address.

Organization Word Clouds

There are different types of word clouds, but one common approach is to generate a visualization that increases the size of a word based on up its frequency. Other aspects such as font style, color palettes, word placement within the cloud, text directionality, layout size, and so on may appear as options depending on the word cloud tool. The first and second word clouds below follow a design

for small word lists.[13] The third word cloud required a different site to handle the large number of 279 uniquely named organizations with organizational frequencies that varied from one to 27.[14] Note, these word clouds use organizations listed by anyone in the tracking data, whether or not they attended the event; so, these word clouds represent more of an interest in the event rather than actual attendance.[15]

Figure 2: Academic Organizations Word Cloud

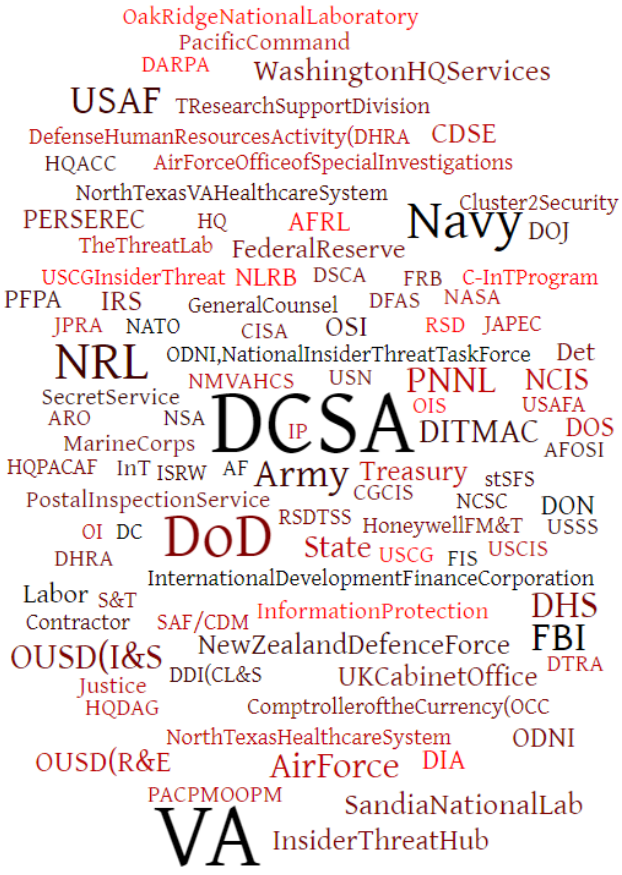


Each of the following word clouds contain words taken from one of the organization groups. Larger font size words indicate more frequent use in that word list. Other than setting the colors used, aspects such as color assignment and word placement using the tool's default values. In some cases, word lists were edited to increase the similarity of the same organization that was spelled differently by different attendees which improves the word cloud performance; for example, many people from ARLIS entered ARLIS as their organization, although some people entered the Applied Research Lab for Intelligence and Security; the latter were changed to ARLIS. Commonly used terms such as "university of" were removed from the academic word list to prevent them from having an overwhelming presence in the word cloud.

Exploring Figure 2 some basic findings emerge. It comes to no surprise that Figure 2's focus on academic organizations shows that ARLIS, the (University of) Maryland, and UMD were the most prominently featured terms. Other major notables included JHU-APL (John Hopkins University Applied Physics Lab), UNC Charlotte, and CMU (Carnegie Mellon University). This cloud also has the fewest number of terms overall, in part due academic attendees having had the smallest portion of total number of individuals in their group.

[13] The first two came from www.worditout.com with iterative generations to increase the number of words included in the word cloud. They use a 5:3 ratio landscape format to form a container space for the words; a 5-color red to black palette with color assignment generated randomly and can fit up to 100 words depending on word size and length.
[14] The third word cloud was produced at www.wordclouds.com, using a full stretch shape, five colors from red to black, a gap size of four, -5 on the scale bar, a 1024x768 [4:3] aspect ratio, and horizontal word direction.
[15] Additional work is needed to further parse the data to obtain attendee-based word clouds. Although such clouds may be more complicated visualizations if also considering degree of participation over the events attended.

Figure 3: Government Organizations Word Cloud



The second word cloud features government related organizations, both military and civilian. ARLIS has growing ties to DCSA given the InR topic that is central to both of us; additionally, one of the IRiSS team is a former DCSA director. Thus, DCSA made sense to be the largest, central term in the cloud. The tangential offices of PERSEREC and OUSD(I&S) were present but overshadowed by other organizations. The VA, or the Department of Veterans Affairs, had a surprisingly large showing at IRiSS events relative to the other organizations, second only to DCSA. This was followed by some of the well-known military groups: DoD, Army, Air Force, and Navy; the Marines are listed but much smaller in the word cloud. Often, these branches appeared alongside other organization names in the data, such the Navy and NRL (Naval Research Lab). The next strata size down contains a large range of organizations, including many civilian. The largest civil groups include the FBI, Treasury, and some of the Department of Energy's national labs like PNNL (Pacific Northwest National Lab) and Sandia National Lab. Interestingly, a couple of the international government organizations were far from the smallest represented, including the New Zealand Defense Force and the UK Cabinet Office.

Figure 4: Profit / Nonprofit Private Organizations Word Cloud

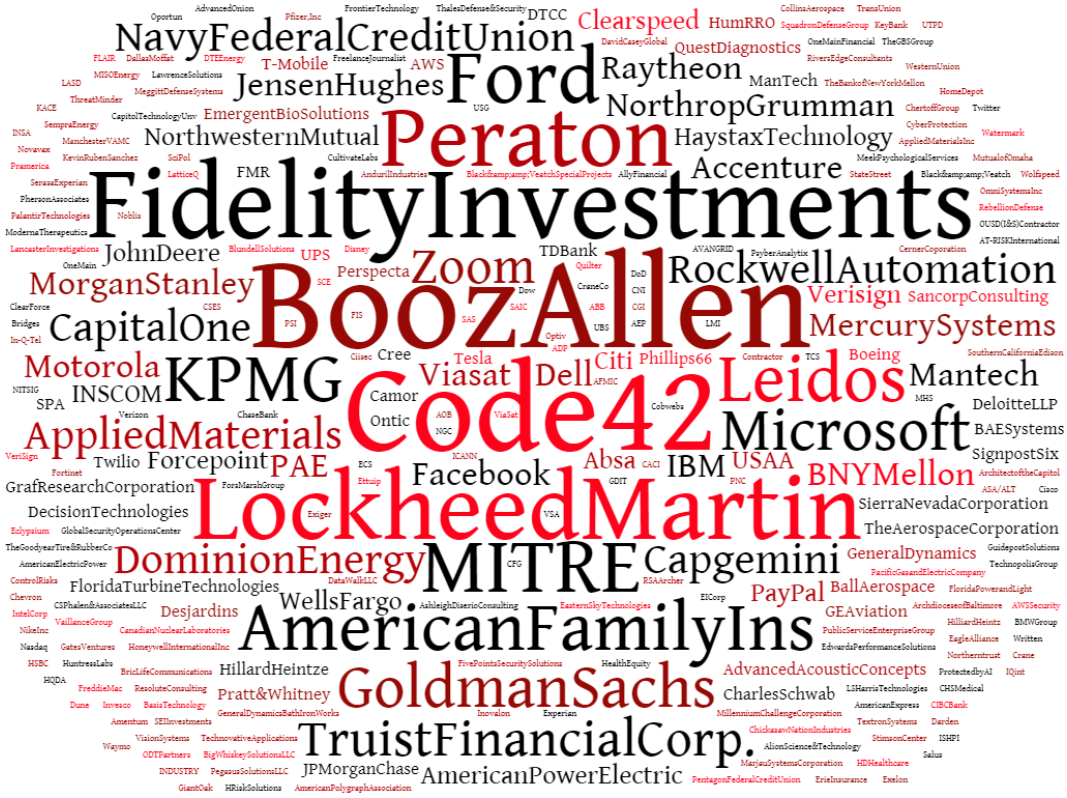


Table 9: Organizations with >5 people interested in IRiSS

Organization	People Affiliated
Booz Allen Hamilton	27
Code42	22
Fidelity Investments	16
Lockheed Martin	15
Peraton	12
MITRE	9
Ford	9
KPMG	8
Leidos	8
American Family Insurance	8
Microsoft	7
Goldman Sachs	7
Truist Financial Corporation	6
Mantech	6

Zoom	6

The third word cloud contains private and nonprofit organizations—279 names in total with frequencies that varied from one to 27. Table 9 reveals the which organizations had more than five people in total associated with that organization who were interested IRiSS events. The top associated organizations offered a range of diversity, showcasing the IRiSS' broad appeal to a wide array of companies. These top 15 organizations spanned management consulting, security services, the defense industrial base (DiB), financial services, motor vehicle production, and technology products. Each of these areas had situated needs and challenges, some of which IRiSS aimed to address through key topics such as industry views and modeling. Additionally, some engagement could have stemmed from having IRiSS guest speakers who were leaders at those organizations, such as Caroline Gilman from Booz Allen Hamilton, Doug Thomas formerly of Lockheed Martin (now at JP Morgan Chase), and Stephen Szypulski from Goldman Sachs. Individuals from these 15 companies totaled 165 people, or about 30% all profit and nonprofit affiliated individuals and about 12.7% of all IRiSS interested individuals.

Poll Feedback

One goal of the IRiSS event analysis was to collect feedback from attendees. An attempt used a Google Form and was test run; however, response results were poor and new approaches to collect feedback sought. It was not until after the fourth IRiSS event that the team learned of real-time polling features that were available in ZoomGov. The team revised a much shorter version of the previous feedback poll, which was implemented for IRiSS events 5 and 6, the results of which appear below. The real-time feedback poll pops up on the attendee's screen. Since it requires use of the ZoomGov app, the IRiSS team believes phone-based attendees that dial in would not be able to use this option.

Tables 10 and 11 each have the same four measures of overall satisfaction, with ordinal scale response options ranging from terrible (one) to excellent (five). Event 5 covered InR, HR, and workforce supply chain challenges. Event 6 was the capstone event on actualizing the InR paradigm. They differed slightly in format such that event 5 had three speakers and ran for 60 minutes, while event 6 had four speakers and ran for 90 minutes. Assuming phone attendees could not take the poll, this analysis used the lower band attendee values from Table 6 above, the feedback participation rates are 42% and 24% respectively for events 5 and 6.[16]

The overall satisfaction results were quite good. There were no ratings of a one or two for either event, except for a single two on event 5 pertaining to advancing the conversation. The remaining scores for both events 5 and 6 gradually increased, and there were clear majorities with the Excellent rating in most areas of satisfaction.

Table 12 offers insights as to the types of organizations corresponding to the attendees providing feedback. This poll question response options doubled the number of organizational groups, offering

[16] They are not statistically different from the organizational groups (USG 34%, private/npo 43%, and academia 13%). Event 5 results: $X^2(df=2, n=73)=5.40$, $p=0.067$; Event 6 results: $X^2(df=2, n=41)=2.32$, $p=0.313$.

two response options for each group type based on the type or relationship with government. Government was not defined and could be conceived at any level.

Looking back to Table 6, group identity was approximately 34% USG, 43% private / nonprofit, and 13% academia. The feedback polls tracked somewhat to those results. Except for a larger proportion of academics providing feedback during event 5, as there were about 1.5 times as many academics during event (21%) compared the overall 13%, the rest of event 5 and all of event 6 matched very well to the overall group percentages.

Table 10: IRiSS Live Poll Feedback - Event #5 Workforce

Rating:	Terrible 1		2		3		4		Excellent 5		Total	
Overall Satisfaction:	**#**	**%**	**#**	**%**	**#**	**%**	**#**	**%**	**#**	**%**	**#**	**%**
Met Expectations	0	0%	0	0%	4	5%	33	45%	36	49%	73	100%
Topic Quality & Organizational Relevance	0	0%	0	0%	4	5%	26	36%	43	59%	73	100%
Advance Conversation in Their Community	0	0%	1	1%	8	11%	23	32%	41	56%	73	100%
Speakers & Overall Engagement	0	0%	0	0%	3	4%	20	27%	50	68%	73	100%

Table 11: IRiSS Live Poll Feedback - Event #6 Capstone

Rating:	Terrible 1		2		3		4		Excellent 5		Total	
Overall Satisfaction:	**#**	**%**	**#**	**%**	**#**	**%**	**#**	**%**	**#**	**%**	**#**	**%**
Met Expectations	0	0%	0	0%	4	10%	13	32%	24	59%	41	100%
Topic Quality & Organizational Relevance	0	0%	0	0%	5	12%	9	22%	27	66%	41	100%
Advance Conversation in Their Community	0	0%	0	0%	9	22%	16	39%	16	39%	41	100%
Speakers & Overall Engagement	0	0%	0	0%	3	7%	13	32%	25	61%	41	100%

Table 12: IRiSS Live Poll Feedback - Respondents' Organization

> "...The ARLIS institution has become one of my preferred organizations for authoritative information and experts on insider risk and other security topics. As a Marylander, it's great to know that UMD is the USG's applied research lab in the field of intel and security."
>
> – *anonymous*

	#5 Workforce		#6 Capstone	
Organizational Representation	**#**	**%**	**#**	**%**
Academia - does not have current / recent funded government security-related research	2	3%	0	0%
Academia - with current / recent funded government security-related research	13	18%	5	12%
Government - agency other than defense-related	8	11%	5	12%
Government - defense-related agency	17	23%	9	22%
Industry / for profit/nonprofit - with government contracts	33	45%	4	10%
Industry / for profit/nonprofit - does not have government contracts	*	*	18	44%
Total	73	100%	41	100%

* *This response option was not included by mistake when first establishing the ZoomGov polling.*

A.3: DIRECT FEEDBACK RECEIVED

IRiSS feedback received via email and chat outside of events. Additional information was not collected along with this feedback.

- The series looks so interesting. Could you keep me in the loop for further discussions? Look forward to learning about your efforts going forward.

- I appreciate this meeting.
- I am very interested in the opportunities to hear some of the speaker series.
- Thanks, and please keep me on the distro lists for future events.
- Great job!
- What a great panel! Good participants and good moderation, and lots of interesting content!
- I found the speakers and all that they had to say extremely interesting, and it was refreshing to hear these issues described from the perspective of insider risk management and not treating this as an adjunct to cybersecurity. [… delete] The overall thrust of seeing this as a human problem and treating people as people chimes very well with our position. We also agree with your efforts to shift the paradigm from countering a threat to managing a risk. This gets our vote!
- Wow, Shawn. Thank you for the information
- Thank you for supporting today's conference. The topic is related to the program I support at [company name] and I found the material extremely useful. […jump to follow-up email] The moment you update the April sessions, I'm letting my team know ASAP. They will really enjoy the content!
- Thank you so much for including me in this discussion today. It seemed like a very engaged audience today which is excellent.
- Thanks for setting this up and allowing me to participate.
- I attended one of these events already and found it really helpful, so thank you for this. I am forwarding the registration information to customers of mine […deleted stuff about event times].
- For this attendee, it was a great panel. Thank you all!
- It was a very enlightening discussion.
- Thank you---I learned a great deal from the conversation.
- I'm out of office next week and super bummed to miss this next speaker topic. […deleted recording request]
- I just wanted to take a second to thank you for compiling and disseminating this information [speaking about a shared reading list on IR modeling] - I'm always on the lookout for high-quality research on insider risk, and specifically on the modeling thereof, and this is going to be immensely helpful. And more broadly, thanks to you and ARLIS for this great speaker series. I've really enjoyed it!
- Powerhouse panels. Great series. Thanks!

> "…I'm always on the lookout for high-quality research on insider risk, and specifically on the modeling thereof, and this is going to be immensely helpful…"
>
> – *anonymous*

> "Powerhouse panels. Great series. Thanks!"
>
> – *anonymous*

"**…**thank you for your passion and your ability to bring together fantastic speakers and community engagement around Insider Risk. Your choice of topics and speakers are really strong and aligned with [… delete company name] vision of Insider Risk and our desire to further educate the security community."

– anonymous

- I really like these IRiSS speaker events – great speakers, interesting subjects and great moderating by your good self. Many thanks again and I look forward to the next one.
- Thank you. My team appreciates these!
- I'm looking forward to next week's session on insider risk and human resources. The ARLIS institution has become one of my preferred organizations for authoritative information and experts on insider risk and other security topics. As a Marylander, it's great to know that UMD is the USG's applied research lab in the field of intel and security.
- First of all, as a participant in many of the ARLIS IRiSS events, I want to thank you for your passion and your ability to bring together fantastic speakers and community engagement around Insider Risk. Your choice of topics and speakers are really strong and aligned with [… delete company name] vision of Insider Risk and our desire to further educate the security community.
- Congrats on wrapping up the IRiSS series! Great content and very well put together.

A.4: QUESTION LISTS BY EVENT

A.4.1: Event 1 Question list

30 March 2021: State of insider threat and insider risk paradigms

Part 1: Insider Threat Retrospective with Doug Thomas & Matt Eanes

1. With a long history of insider threat work behind us, what have we learned so far? What still puzzles us?
2. What risks do you think the current system of insider threat is best at detecting, and which ones do you think it's more likely to miss?
3. What do you think are the top 2 or 3 things that create or maintain an appropriate awareness (& mitigation) of insider threat within an organization?
4. What are key strengths to the current Insider Threat paradigm/approach that should not be left behind? What metrics matter most today and should be brought into tomorrow?
5. How do you describe/define success in Personal Security--for Personal Security Clearances? How do we know we have achieved it and how do we adjust for failure? What are the measures of effectiveness and efficiency?
6. If/when we cannot show empirical evidence (causation and/or correlation) stemming from steps we take in Background Investigations, what is the rationale for the steps we do take?

Part 2: Insider Risk with Natalie Scala & [4th Guest Speaker, name redacted]

1. Insider threat is called a "user problem", whereas insider risk is a "data problem". What changed to shift this problem focus and what are the great insider risk puzzles that emerged from this shift?
2. What do you think are the top 2 or 3 things that create or maintain an appropriate awareness (& mitigation) of insider risk within an organization?
3. What are the biggest things you would change about the current approach(es) if you were designing an insider risk system from scratch?
4. Where do you think AI/ML can have the biggest impact in moving to Insider Risk? What worries you the most about AI/ML applications to Insider Risk?
5. How can (should? must?) we appropriately target our Insider Risk detection/mitigation efforts while maintaining diversity of (and fairness across) our workforce community?

Part 3: Everyone returns for 1 final question

What do you think will be the biggest differences between Insider Threat today, Insider Risk tomorrow, and Insider Risk in (say) 2035?

A.4.2: Event 2 Question list

Monday 26 April 2021 @ 13:00-14:00: From threat to risk: Gain & loss, response, and management around insiders within academic environments

For all questions except the first, we focus on Insider Risk as we want to orient the conversation to risk thinking, but there is room for Insider Threat if you want to differentiate your responses.

1. Let's get a little warmed up. What does Insider Risk mean to you and how does it differ from Insider Threat?
    - Do you have a better term that represents where we are, or should be, regarding an approach perspective to preserving the integrity of research, facilities, and people within your academic institutions?
2. Can you give an example where current Insider Risk requirements helped prevent integrity loss of research, facilities, or people?
    - Were any of the successes 'pyrrhic victories' where the costs to the research were excessive?
3. What have been the greatest 2-3 challenges with onboarding the research community, including faculty and students, within your institutions with Insider Risk awareness? What did or did not work well from those challenges?
4. What are your thoughts about insider issues that result in integrity loss of some kind to domestic, rather than foreign, organizations?
    - Any thoughts or concerns about foreign influence operating through a domestic organization?
5. From the perspective of Academia, how well do the DoD, FBI and Homeland Security work together to support the interests of the US Government in Academia? If their relationship is not optimal, what would make their relationship optimal for Academic Institutions?
6. Does the US Government provide your institutions with a single picture of comprehensive risk facing your Academic Institutions?
    - These would include threats such as methods employed, adversaries approaching, information targeted, as well as vulnerabilities and consequences.
7. Ok, last bit from me—I have two scenarios, one for each of you.
    - Dr. Laurie Locascio – It's 2035, and your ideal academic "Insider Risk" ecosystem is in place. What does it look like? What were instrumental steps to get there?
    - Dr. Kevin Gamache – It's 2035, and things have gone horribly wrong for academic Insider Risk. What does that look like and what might have caused that to happen?

A.4.3: Event 3 Question list

Tuesday 25 May 2021 @ 10:00-11:00: Industry views – Where are we now

For all questions except the first, we focus on Insider Risk as we want to orient the conversation to risk thinking, but there is room for Insider Threat if you want to differentiate your responses.

1. Let's get a little warmed up. What is the difference between Insider Risk and Insider Threat?
    Possible probing questions:
    - Threat and vulnerability? Risk and consequence?
    - Do you have a better term that represents where we are, or should be, regarding an approach perspective to preserving the integrity of people, facilities, and other forms of property and processes within your organizations?
2. What should companies do to build more trust and resilience at work? Can you give specific examples?
    Possible probing questions:
    - What is your company doing to build more trust and resilience at work?

    - Is your company developing a corporate culture of insider risk, and if yes what is a top activity for its success?
3. To what degree is your company thinking about insider risk as part of a larger ecosystem of potential failure modes? What role has company culture played establishing this way of thinking?
4. What is one thing you'd like to share about insider risk from your industry that you think other sectors of industry are not doing or doing well?
5. If you could offer one best practice or other takeaway from industry for your government counterparts working on insider threat / insider risk, what would it be?

If time allows:

6. How do you describe / define success for mitigating / managing insider risk?
   Possible probing questions
   - What are the measures for effectiveness and efficiency?
   - How do you adjust for shortcomings?

A.4.4: Event 4 Question list

Tuesday 29 June 2021 @ 12:00-13:00: Tools, methods, and technology -- State of the art in modeling

1. How do you describe/define success for modeling insider risk? How do we know we have achieved it? What are the measures of effectiveness? What are the measures of efficiency? How do you adjust to shortcomings?
2. In your view, are the tools and technologies we have available today for modeling insider risk sufficient? What are they doing well? What are they missing?
   - Probe: To what extent are existing tools tested or proven to be effective?
3. What do you think current insider risk modeling efforts are best at detecting, and what are they more likely to miss?
4. Where do you go to find new information so you can update insider risk modeling efforts? How do you adapt modeling concepts and emerging developments to obtain new models?

5. When it comes to insider risk processes, who in the organization could benefit the most from communicating more with modelers? Conversely, who should modelers communicate with more closely in their organizations?
6. *If time permits:* Can you tell me about a time when upper management instructions challenged you to update or apply insider risk models? What did they ask of you and how did you overcome it or why did it fail? If you were the upper management sending the instructions, what challenges were you aware of that would be faced by your modelers?

A.4.5: Event 5 Question list

Thursday 22 July 2021 @ 12:00-13:00: Insider risk, human resources, and the human capital supply chain challenge

1. How do you describe/define success for insider risk with respect to hiring and vetting within our workforce supply chain? How do we know we have achieved it? How do you adjust to shortcomings?
2. When it comes to hiring and/or vetting, what risks do you think the current system is best at detecting, and which ones do you think it's more likely to miss?

3. To what extent are hiring managers, personnel vetting, and counter insider threat/risk people talking to each other about hiring practices? What improvements do you think can be made here?
4. Have you or your HR/vetting/hiring colleagues discussed workforce supply chain or other organizational challenges associated with not hiring select individuals or groups of people? If so, can you give a brief overview of the challenges or impacts discussed? For example, you might have a highly qualified computer programmer or other special skillset but has a criminal conviction or other potential risk in their background.
5. Have you or your organization had to hire large groups of people within a short period of time? If so, what was this experience like with respect to consideration to Insider Risk? What, if anything, did you change about the hiring processes?

Additional questions if time permits:

6. How, if at all, are you leveraging AI/ML to assist with hiring or personnel vetting toward Insider Risk within your organization? Have any human resource related concerns emerged related to using AI/ML for hiring or vetting?
7. If/when we cannot show empirical evidence (causation and/or correlation) stemming from steps we take in security screening for hiring or vetting, what is the rationale for the steps we do take?
8. If you could offer one best practice or other takeaway from a human resources lens for your government counterparts outside of human resources working on insider threat / insider risk, what would it be?

A.4.6: Event 6 Question list

Tuesday 17 August 2021 @ 12:00-13:30: Actualizing the Insider Risk Paradigm

Each previous IRiSS event generated a series of takeaways. Below is one takeaway selected from each previous event. I will pose each takeaway to the panel and ask each of you to react to the takeaway.

Example responses might include if you agree or disagree with the statement, how might you expand or change it, or how it might be relevant as part of the bigger picture in shifting the dial from Insider Threat to an Insider Risk paradigm.

Topic Areas

1. (Kickoff event) The shift from Insider Threat to Insider Risk must include a narrative change requiring empowerment, trust, and sociotechnical solutions without being singly reliant on people or technology.
2. (Academic environments) Collaboration between the research community and security remains a great challenge and natural friction source [*moderator to insert example such as sometimes we don't speak the same language or have the same priorities in terms of benefits, intent, purpose, reputation, etc.*]; more and better risk/impact data can help bridge difference in priorities between these groups.
3. (Industry views) Some of the best actions are designed to be pre-emptive: sharing examples of good outcomes, strengthening leadership support and partnerships with government and across industries, expanding equity, diversity, and collaborative professional programs within the organization.

4. (Modeling) Need to focus less on the individual, more on context; less on process, more on outcome; less on easy but less valuable models, more on thoughtful model design and sources of information.
5. (Workforce supply challenges) Insider Risk programs should span from hiring to separation; hiring and continuous vetting benefits from deliberative, proactive, collaborative engagement between HR, legal, security, employee relations, and other relative departments and stakeholders.

A.5 EVENT SUMMARIES

All six summaries here have approval for public release.

A.5.1: Event #1 Summary: State of insider threat and insider risk paradigms

ARLIS IRiSS Event Summary

30 March 2021: State of Insider Threat and Insider Risk paradigms

In this event, ARLIS featured four guest speakers: Doug Thomas, Dr. Natalie Scala, Matt Eanes, and [4th speaker name redacted] (speaker titles and bios appear on the IRiSS website event description). They responded to a series of moderator questions they received in advance along with and real-time questions posed by the event attendees. This summary is a high-level overview of responses to those questions. After each part within the summary, a list of the question themes helps illuminate interests from the attending community. To help shorten the summary length and distinguish responses from the speakers and attendees, contributing conversation from the ZoomGov attendee chat is omitted.

Executive Summary

The overall themes that emerged pertained to issues of complexity that are inherently built into the human domain, which, in turn, affects our current metrics for effectiveness, and the need to foster individual and team support within an organization. The paradigm shift from InT to InR is not just a wording change or looking at a different type or source of data. The shift is also a narrative change that requires empowerment, trust, and sociotechnical solutions without being singly reliant either on people or technology. Yet even a full pivot to InR may not be sufficient to maintain security for our people, organization, customers, and sensitive, proprietary, and intellectual property. InR is a good, next step from InT but not the final one. The values and measures needed to continue this evolution will require ongoing conversations and research as we move the dial from problems to solutions. As we look to the future, many contributing norms and values, such as those related to privacy, will continue to affect InR work, but the degree to which those norms and values continue to contribute may largely depend on their changes over time.

Summary

Part 1: Retrospective on Insider Threat - Where we were and are today

Featured speakers: Doug Thomas & Matt Eanes

Looking back on what we learned about InT. CInT is a team effort that relies heavily on understanding work culture and training. Hiring the right people for the mission plays a large role, but so does supporting those people. Part of supporting your people includes a needed shift from a compliance-based model to a risk-based model. Much of this shift stems from a need to better understand our environment and the people in it since human behavior and activity spaces such as social media remain a mystery. Proper awareness for InT remains key. Such awareness comes from proactive internal communication and demonstrating values of honesty, transparency, and fairness. Myths that perpetuate a sense of invulnerability within the organization reduce awareness.

Understanding success regarding personnel security. Being successful with InT, and more specifically personnel security, can mean different things. There is the usual approach of being good at collecting metrics based on costs to obtain them, and we understand cost-based metrics well even if we struggle with timeliness and determining how we measure effectiveness. This includes things like mobility, how quickly we can get trusted people in the door or move them around with the least amount of friction, and ensuring that our background processes align with the mission. Overall, to be successful we need to create better insights which points us back to our use of data and metrics.

Key strengths to the current InT paradigm/approach that should not be left behind and metrics matter most today and should be brought into tomorrow. Our current systems for InT and personnel vetting are good at looking at hard data and using technology to uncover patterns. This is particularly useful for creating metrics for things like file recovery and damage assessments. However, these same systems struggle with soft data, such as human behaviors. Furthermore, unintentional and accidental bad behaviors are hard to proactively combat. These data challenge areas highlight that we should not rely on metrics which focus solely on the digital data, but design them to focus more on human potential and behavior. Metrics should arise from conversations between different components within an organization that consider human risk as a connective tissue, something to be maintained and managed.

Additional responses to other attendee themes: Human resource (HR) related topics were an emerging trend from the attendees. It is possible to bring HR closer to InT processes such as background checks—some organizations are actively doing this. Greater alignment with HR could include a focus on rapid vetting on the front-end and shift from continuous evaluation (CE) to continuous vetting (CV). These issues play into concerns about radicalization and reputational impact on the company, but there is belief that we have largely accounted for radicalization now although there is subjective determination on whether to report. From there, matters such as radicalization and impact should be part of bigger conversations, but these topics tend not to be narrowed enough at the operator level and so it becomes a matter of where and how to focus these conversations within the organization. Potentially, having someone serve as a Chief of Counterintelligence / Insider Threat would help shed light on this portfolio of issues and help set organizational strategy, the necessity of having this Chief role would depend on the individual company.

<u>Moderator question themes</u>

- Major puzzles within InT
- What are we (not) good at detecting
- Appropriate awareness
- Key strengths and metrics that matter
- Being successful

<u>Attendee question themes</u>

- Radicalization
- Human resources (HR)
- Background checks
- New InT positions
- Formalization of InT processes

<u>Part 2: Current and future state of Insider Risk - Why do we need a pivot</u>
Featured speakers: Dr. Natalie Scala & [4th speaker name redacted]

The shift from InT to Insider Risk—focus change from InT called a "user problem" to InR is a "data problem" and emerging puzzles. There are several reasons why the paradigm shift from InT as a *user problem* to InR as a *data problem* started and continues to transition. We start with the recognition that words matter, and the term "Insider Threat" carries negative connotations implications implying that the threat was not only tangible but ultimately unavoidable. Though we are currently shifting to using InR now, the next steps to evolve should move even further 'left of bad' (interventions occur prior to the onset of a bad behavior/event/issue) to pre-risk approaches such as Insider Support, Insider Protection, or Insider Wellness. Such changes happen through largely reactive, but increasingly proactive, policies, like those for the data protection, privacy, and centralization. From here, some of our biggest challenges moving forward with the shift to InR requires answering fundamental questions such as what is the organizational purpose of such programs, what data are they protecting, and what security is used and needed.

The top things that create or maintain an appropriate awareness (& mitigation) of InR within an organization. Part of the shift to InR requires sufficient awareness and mitigation. Awareness is like a vitamin which must be taken regularly so people are aware of inherent risks. Creating and maintaining awareness comes from: educational efforts, everyone taking security seriously, trusting and empowering insiders to do good rather than discouraging them to do bad and fostering positive feedback loops when issues arise. These elements should be both integrated and mutually beneficial to each other, and produce and reinforce mitigation efforts by being simple, direct, and objective.

Biggest things you would change about the current approach(es) if you were designing an InR system from scratch? We should start by acknowledging there are no perfect InR programs. However, there is plenty of room to empower insiders as part of the solution while also ensuring those insiders are not nefarious. Policies should start and continue to address "work arounds" and other behaviors that (unintentionally) increase risk. Additionally, InR programs should not operate in a (security) silo—they need partnerships and collaboration with numerous departments such as HR, Legal, InfoSec, Physical Security, Diversity & Inclusion, and Internal Comms to name a few.

Role and worries about use of AI & ML for InR. Technology is helping rapidly advance InR methods and tools. Artificial intelligence (AI) and machine learning (ML) work receives massive amounts of funding for InR solutions and is making strides to analyze vast amounts of complex data and formulate new research questions. Yet, many insider problems are not getting solved or are growing worse. AI/ML are good at helping establish behavioral patterns and find anomalies, but commonly fall short on predicting intent. There are often challenges with social bias and bias within the data and algorithms. Some AI/ML usage can benefit from measures for behavioral intent, previous experience in the field, and years of cyber education; on the flipside, demographic data should not be used unless necessary. Using this type of data sends a message of non-trust to the workforce and feeds the growing concern for more privacy, even from internal employees. A movement to more privacy-focused data uses and retention is likely to continue into the foreseeable future. Furthermore, AI/ML users should discuss the potential for unrealistic expectations for the predictive aspects and when to couple with other data and explore cases in greater detail. Where InT first shifted the perspective from 'Threat' to 'Pre-Threat', which we called 'Risk', and InR is now

shifting the perspective from 'Pre-Threat' to 'Pre-Pre-Threat', the next step will be a 'Pre-Pre-Pre-Threat' series of detections and analysis, all based on AI/ML, which is likely to be based on relatively weak analysis due to lack of concrete datapoints that are clearly indicative of risky or threatening behaviors. Despite the AI/ML analytical boost, we should avoid putting all of our technology eggs in one solution basket or ignore human solutions. There needs to be a balanced sociotechnical approach.

Additional responses to other attendee themes: Looking to the human elements of InR, the most critical elements include leadership, open admission and acknowledgement that risk exists, being proactive in our approach to addressing and engaging the workforce, and a willingness to take on hard problems. Hard problems include determining which behaviors are nefarious or not, mitigating accidental mistakes, and ensuring insiders are educated on detection and mitigation.

Matters of maintaining diversity and fairness (D&F) arose throughout this part of the event and attendee interest (*Note: some organizations refer to this as diversity, equity, and inclusion, and may have C-Suite role specifically to address these considerations*). In some cases, policies and technology use exacerbate D&F challenges for targeting InR efforts. So many of the views on D&F echo back to other areas of discussion. Targeting programs with respect to D&F should examine organizational values and needs, consider investments and resources, and be strategic with wording choice. Approaches mentioned above to improve awareness are also useful for issues of D&F.

<u>Moderator question themes</u>

- Causes for the threat to risk shift
- Major puzzles within InR
- Creating & maintaining appropriate awareness
- Designing InR systems
- Diversity & fairness

<u>Attendee question themes</u>

- AI / ML
- Social bias
- Critical human elements
- Diversity

<u>Part 3: Bridging threat to risk</u>

Featured speakers: Doug Thomas, Matt Eanes, Dr. Natalie Scala, and [4th speaker name redacted]

The future of InR. With all four speakers on this part of the panel, we started with a look to the future—a prospective on where we will be in 2035. Technology and use of data remained consistent themes. Technology will continue to change the game and boost our ability to extract information, but we would benefit from a focus on the ability to detect information. Our use of technology will get better, but so will use of technology by others against our efforts. Moreover, available data for this work will depend heavily on the desire and capacity for privacy; such issues are prevalent now and seem likely to remain that way. The adage of knowledge is power will move beyond data to incorporate more awareness, which will produce better results and in-turn will help develop more mature programs. One area of this maturity will include improvements at integrated layering our use of technology and trusted insiders, and we will use trusted insiders to boost engagement and education of our employees to report if/when they think they might have been targeted. The future

may also carry impacts from unknown events. Even now, we are still discovering and working through the impacts of COVID, which forced higher rates of online, remote work that may complicate the insider problems and we lose out on some of the human data. One hopeful note is that despite this high rate of unanticipated remote work we have yet to hear of any major breaches.

Additional responses to other attendee themes: Topics of interest from the attendees focused on process and human activities. Attendees gave a sense that our connected systems and hyper-empowerment of individuals could serve to increase the number of risk vectors, particularly among unwitting employees. This makes the development and researching of sociotechnical solutions even more important now. Raising and maintaining ongoing awareness, not just for the unwitting, is one approach to offset the increasing number of ways things can go wrong. Awareness and making problems directly applicable to employees should be part of educational efforts so that they can build and be a part of solutions for themselves. This increases engagement and buy-in which in-turn can help reduce distractions and mutually improve trust. One focus should be on why we should trust someone rather than the security-minded default of finding reasons to not trust someone. The Roger Mayer trust model was referenced, where trust is influenced by integrity, benevolence, and ability, as well as individuals needing to be vulnerable with the things they find important. One more specific risk vector mentioned was social media. When it comes to proactive use of social media in vetting and evaluation, invasion of employee privacy sends a message of zero trust. Instead, it is better to foster an environment where employees will not feel the need to hide anything. Use of CE/CV can help find indicators we would previously miss, but it captures only some portion of behaviors.

In closing, we should think of people less as a problem set and more as a solution set. Bring our insiders into the solution space, in part through raising awareness and improving organizational culture, will help move us from a culture of insiders as threats to insiders as part of our defenses. One example would be fostering an environment where people can be more involved creating those defenses, above and beyond just reporting on others' bad behaviors at work. This employee involvement in designing sociotechnical defenses would generate a sense of community and belonging. Part of this cultural examination should consider the language we use to talk about risks, and the approaches we employ to defend, our companies, communities, and national security from trusted insiders.

Moderator question themes

- Biggest differences now and in the future
- Final thoughts

Attendee question themes

- Continuous evaluation / continuous vetting
- Risk for unwitting threats
- Proactive use of social media

A.5.2: Event #2 Summary: Gain & loss, response, and management around insiders within academic environments

ARLIS IRiSS Event Summary

26 April 2021: Gain & loss, response, and management around insiders within academic environments

This ARLIS event featured two guest speakers: Dr. Laurie Locascio and Dr. Kevin Gamache (speaker titles and bios appear on the IRiSS website event description). They responded to a series of moderator questions they received in advance along with and real-time questions posed by the event attendees. This summary is a high-level overview of responses to those questions. Following is a list of the question themes to help illuminate interests from the attending community. To help shorten the summary length and distinguish responses from the speakers and attendees, contributing conversation from the ZoomGov attendee chat is omitted.

Executive Summary

This event focused on issues of InR within the academic environment. The session had a highly engaged audience and the speakers largely agreed with each other, building upon each other's detailed responses. Lessons learned include that collaboration between the research community and security remains a great challenge and natural friction source; more and better risk/impact data can help bridge difference in priorities between these groups. External relationships with government partners are critical, mutually beneficial, and evolving as we learn from each other; and unlike government and industry relations, copy & paste best practices does not work. Also, when InR programs are working well, it will be like a good cybersecurity program: invisibly running in the background, but massive failures can result in lasting damages to an ability to innovate at individual academic, university, and national levels.

Summary

The event started with a baseline to understand our speakers' thoughts on InR and how it differs from InT. Both speakers use a widely accepted definition of InT as the foundation (ref. CMU SEI link), InT centers on the individual as a threat source of organizational damage and the solution is to eliminate the threat, which does not work well for the individual or organization. One speaker's metaphor provided the internet as a threat which is eliminated by unplugging the computer, but then you don't have internet. Conversely, they saw InR as a more balanced approach looking at risk and benefit with an understanding that there will always be risk and so we use controls to manage it. InR is more data centric, refocusing from centering solely on the individual to a more holistic approach of understanding data risk. Neither speaker had a better term for where we should be than InR; however, suggested that we should maintain risk awareness rather than risk aversion, particularly within an academic community. Moreover, InT terminology and programs that focus on the individual, as reflected in some mandates with DoD or DoE, set choices that make the academic community ineffective and are dangerous to a university.

InR requirements can help prevent integrity loss of research, facilities, and people. There isn't much that is black and white in InR; every risk we evaluate comes wrapped in a shade of grey. Each of us represents some level of InR and there are many ways to find warning signs. There are no absolutes and sometimes knowing the direct consequences of actions is preventing something. For example, an agreement externally vetted was turned down because a subsidiary was associated with human rights violation and turns out later that the company had a known history of tech theft. University

research offices also help investigate integrity issues of bringing non-contracted data between institutions.

Yet, InR results vary and successes resulting in pyrrhic victories, where the costs to the research were excessive, remain a regular challenge. Pyrrhic victories are huge in the academic community. They are a challenge unique to the academic research enterprise given a foundational principle is sharing information. Every security policy must account for this organizational and operational design. Every agreement we pass on can alienate the country or collaborator or can devastate an academic career. Success is protecting the person, university, country, but we never know in the moment all the consequences and the size of the victory. Focusing on the individual is problematic as most InT 'indicators' from industry and government are the expected behaviors of academics. Another focuses heavily on foreign born individuals and the potential for foreign influence, and yet 30% of US Nobel prizes are won by foreign born but US educated researchers. Ultimate pyrrhic victory is the problem of higher education – do not stifle the research enterprise.

Integrity loss is often discussed in terms of InR from foreign influence, but it can happen from US domestic sources as well. It is a balancing act to train individuals who may become future competitors, but there is an expectation for those individuals to innovate rather than clone the research. Although researchers tend to be good at protecting their info information to avoid being scooped. Yet, intellectual property is still stolen, regardless of whether it goes to Idaho or Italy. So, it remains important that InR management processes, like collaboration and Conflicts of Interest, are organizationally agnostic. If a foreign government operates through a domestic organization, it would be hard to know and it helps to coordinate with other academic institutions.

Onboarding the research community regarding InR awareness and have people accept it as a real risk remains a salient challenge. One speaker went further, claiming there is no greater challenge than securing research enterprise without interfering with collaborate culture and innovative enterprise. Security policies largely operate in the background, such as vetting collaborators. Sometimes this requires risk mitigation decisions the research community does not like. This is complicated sometimes by a lack of understanding or acceptance that the threat may outweigh benefits of open research, collaboration, and the free exchange of ideas. Communication here is key, supported by data to justify InR decisions and discussed in ways to account for academics' different priorities, such as loss of grants rather than intellectual property, how to communicate without being isolationist, and value our international collaborators and science community.

Relationships with US government security agencies, such as the FBI and DCSA, are critical to InR success within academic environments. Substantial, mutually beneficial partnership efforts on both sides cultivated a sense of trust and truly collaborative culture. These efforts are long-standing over many years and joined by universities across the country. Despite mutual interests between academia and national security, natural friction remains due to different their missions. Both sides continue finding avenues for complimentary fit and coordination. Active engagement helps government understand how academic culture differs from industry—copy/pasting practices and polices across sectors does not work. Developing InR programs individually is very costly, and

academia benefited greatly from its security agency partnerships with enhancements in areas such as personnel vetting and risk assessment; yet there is still room for improvement, particularly with getting ahead in global competition.

The US government requires disclosure about funding from foreign influences and a 2020 Department of Education report from detailed substantial shortcomings in reported funds. One speaker's university was one of those asked to become compliant, but the non-compliance was not nefarious; rather, university administrators found the way the rule was written made it hard to report. They are now compliant and focusing more on compiling federal laws. Transparency is fundamental for risk awareness. The issue is not about a faculty member having a foreign talent contract, but rather the lack of transparency regarding that contract.

Balancing between InR needs and faculty interests for free and open expression might give the impression of Big Brother. This impression is avoidable by having every PI involved in the InR process. Training is highly effective, improving their risk knowledge and detailing consequences helps mitigate risk. Bring the academic community together on InR and being vigilant. Included in training should be clear IT policies and expectations, particularly regarding any monitoring. The balance line is also seen as an amount of risk tolerance, which differs by institution and cannot be a blanket policy. The funder, nature of research and personnel involved, reputational risk, risk to students, and loss potential and impact can all affect tolerance, creating a mosaic of cases. Regardless of risk tolerance, it is helpful to proactively reach out to reach out to researchers who are in areas that are high risk or have relationships that are high risk for additional training one on one training. Provide allowance for Q&A; faculty tend to become ambassadors to other faculty. The process is quite intensive but prevents the 'checkbox' mentality and improve coordination.
A final InR scenario in the year 2035 allowed the speakers to illustrate how things could go very differently. One speaker addressed an ideal outcome where a strong InR ecosystem felt invisible. Awareness, updates, and training kept everyone current and without feelings of paranoia or distrustful; it is an open and collaborative time where everyone plays their part. The other speaker painted a grim vision where the US academic research enterprise is no longer the best in the world and the US economy is no longer the strongest. The linchpin was universities' failure to address foreign influence challenges with significant cascading loss effects of research data and expertise. Also contributing, Congress legislated solutions that didn't fit the unique academic environment, which stifled the free flow of information and ideas that were the hallmark of universities for centuries. We lost an ability to innovate.

<u>Moderator question themes</u>

- Differentiating InT and Risk
- Preventing loss & pyrrhic victories
- Challenges with onboarding the research community
- Domestic, not foreign, organizations
- Relationships between academia and US federal security agencies
- It's 2035, what happened.

<u>Attendee question themes</u>

- Funding and foreign influence
- Security without being Big Brother
- InT, poorly named concept
- Risk tolerance
- Moving data between institutions
- Lack of trust
- Checkbox training and attitude and behavior change

A.5.3: Event #3 Summary: Industry views

ARLIS IRiSS Event Summary

25 May 2021: Industry Views

This ARLIS event featured three guest speakers: Stephen Szypulski, Caroline Gilman, and Dr. David Mussington (speaker titles and bios appear on the IRiSS website event description). They responded to a series of moderator questions they received in advance along with and real-time questions posed by the event attendees. This summary is a high-level overview of responses to those questions. Following is a list of the question themes to help illuminate interests from the attending community. To help shorten the summary length and distinguish responses from the speakers and attendees, contributing conversation from the ZoomGov attendee chat is omitted.

Executive Summary

This event focused on industry views with panelists providing insights from their own organizations as well as experience gained through collaborations. The session was highly interactive and even when the speakers did not agree on a given topic, areas of overlap were apparent suggesting common approaches. Lessons learned included that industry is generally good at understanding risk widely, so thinking about InR as part of the larger risk ecosystem allows use of a wider range of management tools, practices, and perspectives. Changes from threat to risk occur through intentional and actionable inflection points that work best as ongoing, supportive, and inclusive initiatives at the organization's grassroots level. Also, some of the best actions are designed to be pre-emptive: sharing examples of good outcomes, strengthening leadership support and partnerships with government and across industries, expanding equity, diversity, and collaborative professional programs within the organization.

Summary

To help with a baseline for our discussion, it is important to understand how our panel distinguishes between InT and InR. InT was seen as micro level, destructive, and event based, personified in individual, intentional behaviors. InR was shared as a macro level paradigm and as a highway intersection analogy using a traffic light as an indicator of risk within the intersection. Risk was also defined as a function of vulnerability and threat. Risk can be managed, mitigated, but also multi-causal and therefore more but it is difficult manage. Moreover, risk and threat have different conceptual and contextual meaning within organizational culture. From a cybersecurity perspective, the term 'insider' is problematic. Who is considered an 'insider'? If you are a cyber organization, being an insider is part of your most important identity; then the notion of an insider / outsider is a barrier to the most effective risk management. Notably, Booz Allen Hamilton (BAH) intentionally started their program with an InR grounding rather than InT.

Our panelists took slightly different positions when we extended the concept of InR as part of a larger ecosystem. One speaker viewed potential failure modes as a crowded field when looking across a whole company; InT is just a part of it, addressed by prevention programs. Another speaker didn't see InT as a failure mode; instead, their company expects employees to maintain long standing

business principles of honesty and integrity—or viewed differently, principles could be seen as managing types of capital: intellectual property, people, financial. The third speaker situated InT as part of an evolving six-step activity / action process. Each stage is part of the ecosystem where teams can seek to mitigate InR.

Flipping the conversation to building trust and resilience (T&R) as work, each speaker offered a mix of insights from their respective companies, but all views centered on the importance of supporting employees. T&R are transient and changeable, improved by clear, transparent, and actionable steps within the organization. T&R starts at grassroots level between employee and supervisor. Build foundations of trust with accountability and promote the business culture. This includes fostering a culture of inclusion, diversity, and addressing equity issues. T&R-building support can happen at inflection points, such as onboarding and promotions. Managers should know and show up for their people, supporting different perspectives and reducing group think. This can be echoed at the team level. At an organizational level, it can develop through tangible and intangible benefits such as wellness programs. All such efforts can have metrics, allowing for accountability reviews. Thus, organizational resilience can be a measurable target. As organizations change, reflect on where and how T&R can be strengthened, let employees know they are supported. BAH moved away from annual assessment to a monthly conversation of constructive feedback and to build rapport; this helped with the move to remote work. Daily successes can lead to long term success but won't without intentional actions to make it happen.

Every good industry panel offers some best practices and other advice. Best practices for government included: be more sophisticated about operational risk, use metrics and sophistication of risk management tools; include diversity and be intentional about how you go about challenging/changing the status quo of programs; and foster collaboration, the better they collaborated in their industry hub, the better they did. In addition, create professional pathways within the organization to target InT and equity, diversity, culture, organizational factors simultaneously with metrics and accountability reviews to ensure those pathway programs are successful. Find opportunities, such as this IRiSS event, to share good, specific program examples, which may help offset potential bad industry or 'Big Brother' reputations. Think beyond budgetary limitations to discover benefits in low/no cost things such as leadership support and partnerships. Try to be forward thinking to be proactive instead of reactive—leverage partnership and do not ignore signals or wait for a technological silver bullet. Develop policies and procedures that provide courses of action when specific event clusters occur, like a guidebook which gives more predictability and reduces managerial burden. Acknowledge your InR program gaps—many programs are relatively new, and it can be hard to show metrics/results, others grapple with the problem of limited resources and where to you focus efforts.

Attendees were curious about the types of products and tools used to address InR. CISA uses granular, climate-style surveys with follow ups that focus on attitudes towards mission, attitudes towards leadership, and fairness within organization. CISA treats culture and InR management as a business line where you have improvement plans. BAH uses a suite of critical tools: monitoring, forensics, case management systems, but they are not end as the tools change quickly, evolving with

feedback. Meanwhile, it remains important to pare down to the informative metrics. Goldman Sachs uses big data analytics and include metrics such as incidents and training, but steer away from metrics on firings. They show success to leadership through value saved in reputational impact and loss of intellectual property, items that do not offer the same traditional measures as other business lines.

Culture and was a recuring InR theme raised by the panelists. Culture-related metrics can be found by working closely with human resources (HR). Seek data from employee assistance programs (EAP), retention of employees, and violations of ethics or conduct codes. Where available, use custom surveys, such as FEDS (an annual federal employee survey), to track trust in leadership, trust in interventions, if organizations live up to their values, and if organizations match up to their public declarations to address employee issues/grievances. Despite established organizational cultures, some insiders may maintain their own agendas. Such agendas may arise based on combination of motivating factors, such as financial, psychological, or situational. Part of the InR job is to learn of those motivations, cultures, and other contributing factors. Juxtapose these factors with resource management challenges—allocate based on insider and other types of threats.

Another area of attendee interest were bystander challenges, which occur where people often sense something's not right with a colleague but usually fail to bring that to an organization's notice. Such events are common in industry, but continuous training helps. Include what is considered 'normal' and provide clear lines of communication for employees to use for reporting. Ensure the training includes empathy for diversity and inclusion issues; empathy in an organization can go a long way. While it is possible that employees volunteer or could be recruited to behave outside the norm, none of the speakers found this to happen in their organizations even with their InT and employee motivation analyses.

Moderator question themes

- Distinguishing between InT and InR
- InR within a larger ecosystem
- Building trust / resilience
- Best practices and advice

Attendee question themes

- Bystander challenges
- Individual agendas
- InR product/tool use in teams
- Metrics for measuring culture
- Gaps in InR programs

A.5.4: Event #4 Summary: Tools, methods, and technology: State of the art in modeling

ARLIS IRiSS Event Summary

29 June 2021: Tools, methods, and technology: State of the art in modeling

This ARLIS event featured three guest speakers: Jeffrey Dodson, Katherine Hibbs Pherson, and Andrew Moore (speaker titles and bios appear on the IRiSS website event description). They responded to a series of moderator questions they received in advance along with and real-time questions posed by the event attendees. This summary is a high-level overview of responses to those questions. Following is a list of the question themes to help illuminate interests from the attending

community. To help shorten the summary length and distinguish responses from the speakers and attendees, contributing conversation from the ZoomGov attendee chat is omitted.

Executive Summary

This session covered a wide range of topics for modeling InR. Much of the focus pertained to successful modeling, understanding what is good, obtaining and adapting new information into models, communication, and understanding boundaries and challenges. Lessons learned include that everyone working on InR should be a modeler, with some degree of conceptual to technical capability. Understanding boundaries on risk conditions and acceptable loss informs discussion of what will be acceptable risk, and this is best guided by leadership. We should broadly seek out new information for models across disciplines, sectors, and media formats; seek to bridge the three investigative tracks – HR, ethics, and security and be inclusive throughout the organization. We need to focus less on the individual, more on context; less on process, more on outcome; less on easy but less valuable models, more on thoughtful model design and sources of information.

Summary

Modeling InR is a journey which occurs within complex environments over time. It is tough to know when we achieved success and therefore harder to accomplish. Thus, obtaining nominal baselines are hard and we need to do better at tracking our efforts and effectiveness over time. Modeling is more successful when we incorporate other disciplines, increase our focus on impact and outcome, decrease focus on processes, and improve the agility and speed of our identification outcomes, while reducing the false alarm rates. We become more effective and efficient when everyone involved seems themselves as a modeler and part of the modeling venture, enhancing problem solving perspectives and cogent outcomes, which should also reduce company resource waste. All involved should understand both threat and impact but separate them in modeling. Useful measures include reducing organizational loss and better decision making. Existing quantitative frameworks can help, such as FAIR or Applied Information Economics, but we need to focus more on the context and less on the individual. Trusted Workforce 2.0 (TW 2.0) will hopefully bring some this needed rigor.

Good technologies help modeling efforts but must be useable by decision makers. Such tools and technologies should account for external factors and have commonly understood indicators. Technologies are even more valuable when they help us anticipate rather than predict and focus more on context. Without context, risk modeling can be self-reinforcing and those that do not sufficiently consider organizational policies and practices can exacerbate risk. The modeling technologies landscape is large and evolving. Some techniques do well to model observable behaviors but less so when mapping to actual behaviors. Critical path models and diagnosticity are important approaches for identifying valuable models and factors, as well as help evaluate sources of information and actionable decision-making speed. Looking for what is different circumstances rather than normal (*e.g.*, a layoff) can help modify sensors before an event occurs. It is possible to use multiple tools in combination, but this requires thoughtful design.

Going deeper into computational modeling, we are moving away from intuition-based models. We can develop theory from modeling and document emergent aspects of threat to understand purpose

behind it and reduce false positives. More traditional computational modeling such as Agent-Based Models (ABM) and system dynamics help to map emergent threats, whereas newer AI/ML approaches focus more on the risk scoring part (Bayesian) probability scores. Newer modeling leverages machine learning and behavioral analytics (such as UBA to UEBA or fraud detection) and there is a sense that we can continue to get better at collecting information and understanding the 'behaviors' they indicate. Yet, we should not lose sight that while modeling helps us look through bigger haystacks, and when we identify a needle, we still rely on human intuition for sense- and decision-making. Treat models as alerts that can be biased and think of them as another smart person on the team sharing their input.

Obtaining and adapting new information allows us to update our InR modeling efforts. Discussion forums, like this IRiSS, and interaction opportunities with academia or industry can offer modeling approach previews and stress testing. Internal employees can also be a wealth of information to learn more about situations, procedures, and practices—be intentional, diverse, and collaborative with them to develop and gain feedback on indicators. Just about any source is a potential information reference, such as books and blogs, particularly those that discuss how individuals cope with change. Having an ongoing, varied, wide intake of new information can help anticipate change. Familiarity with PESTLE analysis and Cukier, Mayer-Schönberger, and de Véricourt's book "*Framers: Human Advantage in an Age of Technology and Turmoil*" were highly recommended.

InR modeling does not occur in a bubble. Modelers should communicate with HR and IT; these groups are key data owners and models benefit from their expertise. Anyone within the three investigative tracks (HR, ethics, security) should regularly also be at a common table to discuss behavior ambiguity. Average workers could strongly benefit from engaging with modelers. This has the added benefit of improving InR perceptions, advocacy, and overall better workplace support. Legal should be included as needed, particularly when models and subsequent decisions become increasingly complex with respect to privacy and rights. Modeling is not necessarily limited to the modelers. Everyone working on InR should view themselves as a modeler, possessing at least some modeling knowledge which can be based on something, such as the adjudicative guidelines, and interpreted through their individual personal perspective (framing). Models are getting sophisticated enough that we might be able to reverse-engineer decisions people made.

Limited resources can affect where modelers draw the proverbial line between what is or is not acceptable risk. Quantifying acceptable risk lines require quantifying acceptable loss. Leadership plays a key role to help set risk appetites, clarify risk condition boundaries, and discuss potential harm to the organization's reputation. Tabletop exercises can be useful to activities to explore these limits. Certain issues, such as extremism or workplace violence, may have their own thresholds; however, there may also be legal considerations as previously noted. Previous baselines are useful comparatives, and these records should be maintained over time.

Challenges can exist when attempting broad or intentional including of organizational factors and cultural information into InR modeling. InT was largely considered the domain of traditional security and compliance, but this does not fit reality well. Risk management is far more

interdisciplinary and the 'not invented here' mentality does not work. Input from other operational and academic fields that help us understand society can help boost decision-making, particularly given the increased speed and volume of data which are shaping opinions and actions. This intentional inclusion also helps understand context, offsetting claims that organizational measures and social factors are hard to quantify. Until we deal with context in modeling, problems are bound to repeat when part of the problem is found in that context.

Moderator question themes

- Success in modeling for InR
- Modern tools and technologies
- Detection and misses
- Finding and adapting new information into modeling
- Communicating with modelers

Attendee question themes

- Where to draw the risk lines
- AI/ML vs. traditional computational modeling
- Role of culture and balance
- Challenges to intentional changes in InR modeling

A.5.5: Event #5 Summary: Insider risk, human resources, and workforce supply chain challenges

ARLIS IRiSS Event Summary

22 July 2021: Insider risk, human resources, and workforce supply chain challenges

In this event, ARLIS featured three guest speakers: Charles Phalen, Heather McMahon, and [3rd speaker name redacted] (speaker titles and bios appear on the IRiSS website event description). They responded to a series of moderator questions they received in advance along with and real-time questions posed by the event attendees. This summary is a high-level overview of responses to those questions. Following is a list of the question themes to help illuminate interests from the attending community. To help shorten the summary length and distinguish responses from the speakers and attendees, contributing conversation from the ZoomGov attendee chat is omitted.

Executive Summary

A successful InR program does not operate in a vacuum and accounts for the whole workforce lifespan from hiring to separation. This becomes increasingly apparent during periods of hiring and continuous vetting. Such processes benefit from deliberative, proactive, collaborative engagement between HR, legal, security, employee relations, and other relative departments and stakeholders. This engagement should have buy-in from top leadership and is useful to help develop an organizational culture of security and reduce workforce alienation. InR, hiring, vetting, and other workforce processes should adapt to account for social and technological changes. Collaborative planning and being intentional, such as recognizing the need for increased diversity, can offset adaptation difficulties. Obtaining useful information for hiring and continuous vetting remains a major challenge, which is social rather than technical, despite access to potentially large amounts of information, such as online activity; however, AI/ML may offer sorting solutions. Many opportunities remain in the workforce supply chain and InR nexus which can be leveraged through collaborative planning, early intervention, and intentionally improving trust within the organizational culture.

Summary

Being successful with InR with respect to hiring and vetting within our workforce supply chain is like the rest of an InR program. It asks the same challenges to prove a negative, prove risk elimination, and minimize false positives. Understand that risk is to be managed and accept that eventually something will eventually happen. A successful InR program requires leadership and governance buy-in across organizational structures. Collaboration and trust open pathways to reduce risk and reduce workforce alienation. InR and risk management, rather than InT and finding the people doing bad things, is one step toward reducing that alienation. Together, develop an executable, periodically reviewed plan to mitigate a spectrum of risk and capacities for change. Include scope evaluation, relevant sources and sensors, regular clearance reviews, and have a plan to deal with risk problems. A successful program manages risk as a word problem, not a math problem, and carries through the whole lifespan of the workplace from hiring to separation.

Our current systems for InR with respect to hiring and vetting are at a crossroads which affect how well we manage risk. Soviet recruitment of US personnel forms the basis for our current system and the 13 adjudicative guidelines. However, the risks have changed; society culture and technology have all changed. We know these changes happens, but adjusting our established systems is difficult and takes a long time, particularly due to high risk aversion, pace of current demands, and an increasing scope. The 13 adjudicative guidelines still offer good parameters for vetting processes and identifying needed information, but the system is cumbersome. Obtaining indicators of carelessness or negligence which can decay over time remains a serious challenge during investigations. The issue is social, not technical. Other people may be hesitant to share, and single source intel is insufficient. Information from outside workplace and recorded spaces is even more challenging. We must incorporate other information. Yet, one challenge is how we include such information, like social media or recommendations, given potentials for accuracy, bias, and misinterpretation. The size and scope of additional information further complicates finding that which is helpful without drowning in data. On the upside, people don't join organizations to betray trust, it decays over time. Places like ARLIS are important to help us think differently about measuring and processing such changes in more effective ways and increasing trust within the workforce to do what is right in increasingly complex situations.

Opportunities exist for greater communication and other improvements between hiring managers, personnel vetting, and CInT/R people. These professionals have difficulty talking to each other and working together, in part as many have different perceptions of their responsibilities and authorities. Current interactions here also largely differ by sector. Private companies may not have access to information available to government, such as arrest records, which change how investigations occur. Internal coalitions across company departments (HR, legal, security, employee relations, etc.) can help information gaps, discuss vulnerabilities, and address information sharing hesitancy. Recuring group discussions build relationships to review hiring process observations, share struggles, develop frameworks to improve vetting and InT/R management program. These groups should have key personnel in different departments for continuity, collaborative sustainability, and access. The DoD struggles with these efforts; feedback loops are not always

effective, and communication is largely limited by cultures of program authority and screening knowledge is limited based on training scope, such as with military recruiters. Overall, there is a need for more preventative, proactive communication.

Not hiring individuals, whether as an active choice or result of poor screening functions, is a workforce challenge. Vetting and other processing time is very important to avoid losing candidates along the way. Screening modernizations make the hiring process simpler and faster, allowing for more diverse perspectives and engaging individuals with unique background and skillsets. This diversity further improves understanding of individual risk and feeds back to continually improve background screening attract more diverse candidates. We must think differently and deliberatively to set new hiring paths and processes. For example, a Harvard study found that non-violent felons with waivers to join the Army on average performed better than their counterparts on measures such as medals and promotions. Yet, there remain situations where hiring individuals with criminal convictions can lead to losing certain contracts. Hiring large groups of people in short periods of time can present their own challenges. Ability for large hires is a function of company resources. Smaller companies may use other companies' contractors, thus relying on others to do the vetting. This can be offset by establishing supply chain risk management working groups, with an InR liaison, to vet companies with contractors and help those companies with vetting processes, create internal NDAs, and establish a security incident vendors model. Regardless of company size and resources, do not cut corners in the vetting process, even with large hiring needs. This corning cutting by the Washington, DC police hiring in the 1980s which saw many bad cops hired serves as an example.

Avoid looking for "ah ha" reflection moments as silver bullets of what HR could do differently with more education by an InR team. Instead, rely on early intervention, incident reporting, and organizational memory to help find and fix an issue before something bad happens. Don't dismiss individual behaviors out of hand and instill a culture of not being a bystander. Build trust within the whole organization to help reduce perceptions of Big Brother. Use collaborative hiring groups to overcome cross-group knowledge gaps, such as HR often lacking knowledge of cleared vs. uncleared personnel needs.

Many recent studies show that InR events are caused by non-malicious employees. More training is not always the solution. Find approaches that find those employee populations. Keep people aware of what mistakes look like as negligence remains the largest issue. Use advances in technology and revamp antiquated systems so that such mistakes and carelessness are not as damaging to organizations.

The line between adequate due diligence and overly suspicious or intrusive vetting and monitoring of potential and current employees may be seen differently depending on organizational culture of security. Moving increasingly toward Insider Trust could affect what security actions are conducted and perceptions of those actions. What is considered being "overly" here is contextual on the individual and the need. The more we can clear false positives and reduce white noise, while

expanding our net for relevant data we can sort into useful information, the better we can narrow on behavior and indicators. AI/ML can help with this.

Moderator question themes

- Being successful
- Detection
- HR + PV + CI communications
- Challenges with not hiring
- Large or rapid hiring

Attendee question themes

- Ah ha moments and education
- Non-malicious activity
- MOEs for initial & continuous vetting
- Line between adequacy & overreach

A.5.6: Event #6 Summary: Actualizing the insider risk paradigm (Capstone)

ARLIS IRiSS Event Summary

17 August 2021: Actualizing the Insider Risk Paradigm

This ARLIS event featured four guest speakers: [1st speaker name redacted], Robert Rohrer, MJ Thomas, and LTG (ret.) Darsie Rogers (speaker titles and bios appear on the IRiSS website event description). This event is the capstone following five IRiSS events—each focused on a key area of discussion. Where previous events asked speakers targeted questions, this event asked speakers to provide reaction-style comments to key takeaways from the previous IRiSS events which were provided in advance; speakers also responded to real-time questions posed by the event attendees. This summary is a high-level overview of responses to those comments and questions. Following is a list of the question themes to help illuminate interests from the attending community. To help shorten the summary length and distinguish responses from the speakers and attendees, contributing conversation from the ZoomGov attendee chat is omitted.

Executive Summary

Overall, the speakers largely agreed with previous takeaways and expanded on them. Major focus areas include heavy reliance on leadership and recognizing the interdependent relationships between security, counterintelligence (CI), human resources (HR), and other departments with recommendations for increased collaboration. Organizational culture and the importance of trust and positive, empowering environments play an outsized but underused role in CInR programs. Echoing throughout the entire session, CInR programs have a dual role as supporting and being supported by people. As such, speakers firmly rooted CInR as human security and identified individuals as the most important focus, juxtaposing to the modeling event takeaway. While these issues remain sociotechnical in complex, multidimensional systems, there was a recuring interest to reduce our reliance on technology—there are no technological silver bullets that produce ground truth. Other key interests included strengthening security and InR efforts by tying them to funding and baking security into contracts with clear consequences. Speakers admitted we have much still to do and acknowledged this event as a robust discussion focused on the right direction.

Summary

Part one – Panel reactions to previous IRiSS Event Takeaways

The five IRiSS events leading into this capstone session focused on the following topic areas: kickoff on changing the InT narrative to InR, academic environments, industry views, modeling, and

workforce supply chain challenges. This section features a summary of speaker comments linked to a takeaway from each of the previous events.

Kickoff event takeaway: *The kickoff takeaway noted that a shift from InT to InR must include a narrative change requiring empowerment, trust, and sociotechnical solutions without being singly reliant on people or technology.* Speaker responses fall largely into three focus areas: the narrative, security, and people and technology. Regarding narratives, all speakers agreed that words matter, but they varied opinions on the extent and impact of which InT and InR terminology mattered. To some extent program implementation may be more important than the terms we use to describe those programs. Yet, terminology can provide program scope, influence indicators and measures used, and shape perspectives about such programs. Incorporating multiple disciplines will also affect terms used and how we coordinate strategy. We can recognize the paradigm shift when we can address systems that fail individuals from individuals that fail systems. The paradigm shift also helps address issues of scale and leaders knowing their people. In addition to the social & technical convergence is a multidimensional security convergence of human, physical, and cyber domains. No program will be successful if it ignores the human domain. Countering Insider Risk (CInR) is largely human security, and any paradigm shift should be rooted in the empowerment, trust, consideration for preemptive and proactive efforts to protect the people. Thus, this is a human problem more than it is tech problem. Tech has its uses, but it still requires people to make the tech useful from development and setup to operation and interpretation. Conversations should consider where we focus our attention, such as the new and growing number of vectors in which people, technologies, systems, and networks can be compromised, as well as how to keep ahead of vulnerabilities in positive ways before others exploit them in negative ways.

Academic environments event takeaway: *The academic environment takeaway noted that collaboration between the research community and security remains a great challenge and natural friction source; more and better risk/impact data can help bridge difference in priorities between these groups.* There will always be healthy tensions between security and academia regardless of CInT or CInR program efforts. Security in the academic environment is largely seen as a black box admin issue rather than security specific. Moreover, organizational culture differences make it hard to share data and address InR issues, even among security and CI professionals. These differences reinforce information insecurity and adversaries benefit from this gap, by reverse engineering stolen tech and research; like baking a cake, you can figure it out by knowing enough of the ingredients list. First step is to admit having a problem. Ongoing, directed, and open communication between groups can help unpack that black box and increase CInR within the environment. Senior leaders must direct, enforce, and assure data is shared in these communications. They can help incorporate lessons from the operations security (OpSec) and intelligence communities to integrate information sharing for better risk calculations. Some speakers favored tying federal funding to security requirements which can motivate InR program dialogue. Researchers may better understand the InR narrative if it is tied to their funding, compromised research, and ability to publish. DoD changes in funding requirements and communication efforts is already receiving buy-in from some academics.

Industry views event takeaway: *Some of the best actions are designed to be pre-emptive: sharing examples of good outcomes, strengthening leadership support and partnerships with government and across industries, expanding equity, diversity, and collaborative professional programs within the organization.* The speakers largely agreed that leadership is one of the core components for the success or failure of CInR efforts. Leaders must support those efforts and ensure everyone in the organization and other relevant stakeholders understand their respective InR roles, areas of overlap across departments, and the larger picture. Make this part of organizational culture. This workforce engagement can foster a sense of belonging, diversity, equity, inclusion, and trust—these elements are essential, not just soundbites. Be cognizant of people and groups that could alienated by CInR programs just as they could be targeted by external influences; do not create additional vulnerabilities. Likewise, be aware of people and groups that are intentionally in high stress situations, such as special operations, and the related inherent risk. While we cannot fully prevent affiliated risks, we can seek to recognize early signs, such as being overwhelmed or disgruntled, and allocated the necessary resources to help our people. For external stakeholders, if InR is not baked into a contract, people will not do it or invest money into it. Ensure contractors have their own CInR measures. Internally or externally, ensure we are not delivering or receiving compromised products, vet the entire supply chain. This may require additional education to better grasp the range of components used in your systems and processes and how they mesh with security and InR. Part of this effort must (re)prioritize security matters. Empowering leaders to do well also means they are widely educated and advised on security and InR issues since many leaders do not have these specialized backgrounds.

Modeling event takeaway: *Need to focus less on the individual, more on context; less on process, more on outcome; less on easy but less valuable models, more on thoughtful model design and sources of information.* Of all the takeaways, speakers seemed to contrast with this takeaway the most. There was general agreement that context remains important to inform how we can better protect ourselves and our people. However, not focusing on the individual was described as counterintuitive as individuals are the key to managing InR and our best source of information. Whether process or outcome, the speakers framed the workforce and work environment as essential elements. Inclusive environments with proud, united, and empowered employees identify and mitigate InR, but can also be useful for modeling discussions. This may help offset challenges with building security models where the whole landscape changes as soon as you have a working model. Thoughtful models benefit from wider engagement to help identify the right amount and type of data needed; enough is needed for security analysis and to motivate people but not so much that people feel untrusted. More attention is needed for modeling at scale, where it is not as realistic to focus on individuals.

Workforce supply chain challenges event takeaway: *InR programs should span from hiring to separation; hiring and continuous vetting benefits from deliberative, proactive, collaborative engagement between HR, legal, security, employee relations, and other relative departments and stakeholders.* On this portion, the speakers agreed entirely with the takeaway, their comments discussing coins, collaboration, and culture. Human threat and human capital are different sides of the same coin. They are both concerned with motivation, ability, opportunity, just for different purposes. Both sides of the InR and HR coin must be involved through the entire employment

lifecycle. We need to build trust into that lifecycle, which can be done through collaborating across departments and with other stakeholders that overlap with InR. Security professionals must understand these interdependent collaborations which can develop better whole-person perspectives. Broad engagement boosts local level and individual engagement, which are key aspects for trust building. These interactions benefit positive organizational culture change, although change can come slowly depending on the organization's current context. Org culture affects everything from recruiting, screening, and onboarding to understanding better ways to adjust resources and capabilities. It is also fundamental for asking how to help others and get others to ask for help.

Part two – Open Q&A discussion

Attendee questions coalesced into three categories: individual matters, things that affect the organization, and improving CInR efforts in general. The first thing to understand about individuals is that it is entirely possible to get 'left of boom.' However, we must see InR fundamentally as a human problem with a human solution and acknowledge our success depends on how well the programs are proactively engaged by the workforce. Technology will never give us the ground truth, so we build a better foundation with people.

Leaders as individuals maintain 100% responsibility for CInR, but they need metrics to help drive change. Help them by being open and seek audits, possibly from outside assessment, that give metrics to know what is strong and where we need to improve. Understanding the impact of not acting applies to both individuals and organizations.

More stick than carrot may be needed to motivate entire organizations and the people within. Carrots involve adjusting incentives and funding requirements to improve security and accountability. Sticks make this clear in contracts and incorporate steep consequences, such as financial or reputational costs, for violating security principles. Design contracts to match threats and risks but understand contracts may become outdated. These efforts should echo through all of your supply chains, acquisition security, and related policies. Collaboration between departments improves ongoing communications and outcomes while breaking down silos. HR, security, and CI, share a symbiotic relationship. Stronger organizational relationships fill information gaps and whole-person concepts.

This series seeks to move the paradigm shift dial from CInT to CInR. Both build on the same model of motivation, opportunity, and ability. Likewise, both can promote and empower the good to prevent the bad. This shift is in-part a cultural one that requires building trust with employees, empowering leaders, and educating stakeholders to focus on a risk environment in which we mitigate the behaviors before they manifest. Some of this should consider American cultural aspects of an individualistic society rather than one that favors the greater environment. Narrative and perceptual changes benefit from increased human intelligence and a reduced reliance on technology. Resources to widely boost CInR efforts are available through the CDSE's trainings and their Sentry app, as well as online information from DCSA, DITMAC, and PERSEREC.

Moderator event takeaway themes **Attendee question themes**

- Narrative shifting
- Natural friction between security and research community
- Pre-emptive actions, leadership, and partnerships
- CInT/R modeling scope changes
- Workforce lifecycle and organizational engagement
- Early employee risk prevention
- Offsetting contractor lack of interest
- InR expenditure justifications
- InT and InR as separate missions
- Recommended InR resources
- How to engage management
- Magic wand – any one change