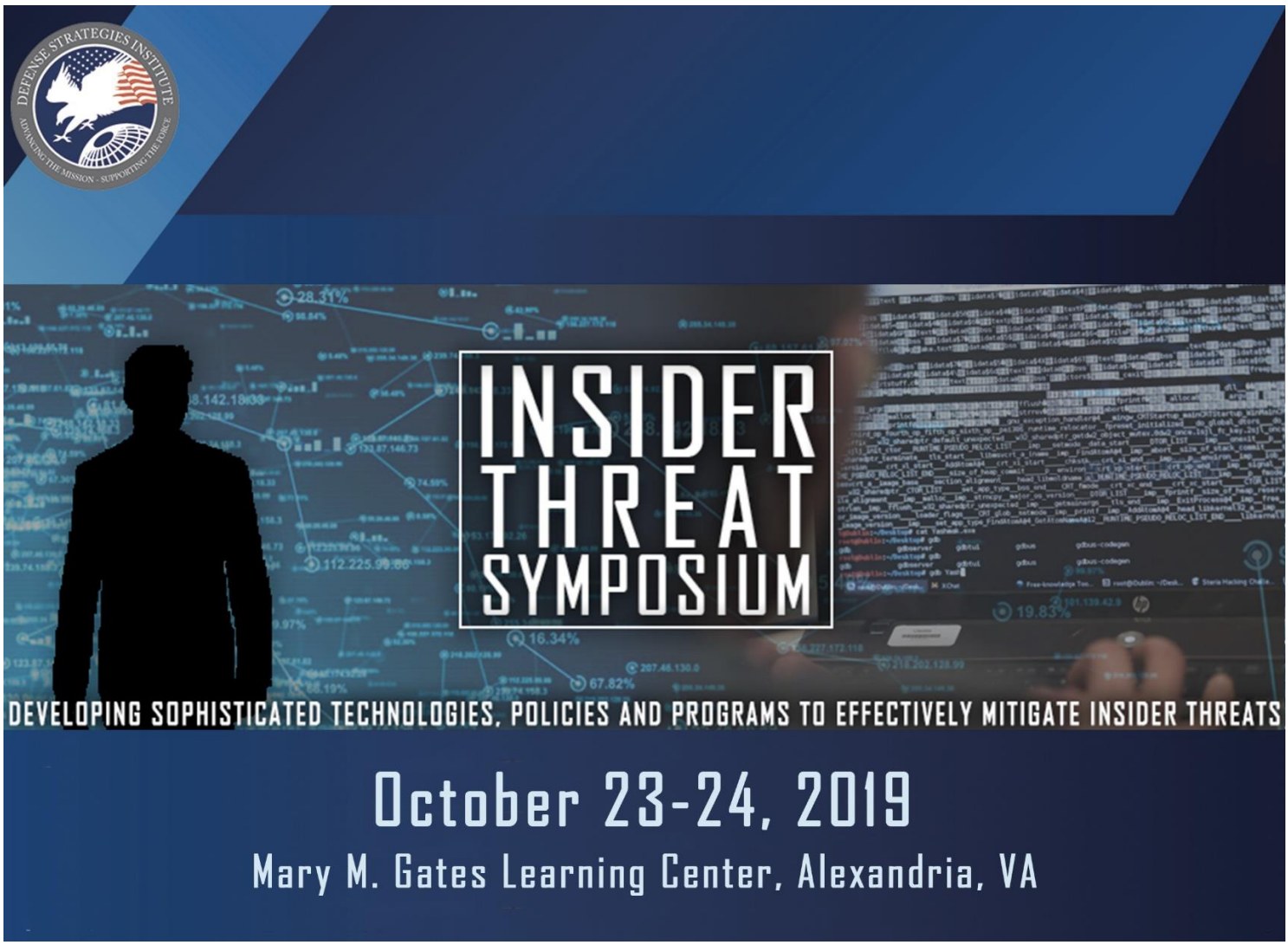
INSIDER
THREAT
SYMPOSIUM
DEVELOPING SOPHISTICATED TECHNOLOGIES, POLICIES AND PROGRAMS TO EFFECTIVELY MITIGATE INSIDER THREATS
October 23-24, 2019
Mary M. Gates Learning Center, Alexandria, VA

October 23, 2019	
8:00 – 8:45	***Registration and Light Breakfast Reception Open***
8:45 – 9:00	**Chairperson Opening Remarks** **Moderator:** **Jim Onusko,** Director Strategic Solutions, LexisNexis Special Services **(Confirmed)**
9:00 – 9:45	**Combating the Threat of Insiders and Unauthorized Disclosures to Protect National Security** - Leading government wide efforts to prevent and respond to the continuous risk posed by insider threat - Mitigating insider threats while also ensuring the protection of civil liberties, rights and privacy - Closing critical CI and security gaps in Executive Branch departments and agencies - Advancing capabilities to combat the increasing sophistication and availability of encryption tools, cloud computing, and malware technologies. **William Evanina, SES (Confirmed)** Director, National Counterintelligence and Security Center
9:45 – 10:30	**Leading FBI Efforts to Detect, Prevent and Mitigate Insider Threats** - Coordinating InT strategies across the FBI - Leveraging behavioral science and situational cues to accurately and rapidly distinguish real threats - Increasing the technological resources and authorities available in order to neutralize national security risks **Jesus Chevere (Confirmed)** Unit Chief, Insider Threat Office Federal Bureau of Investigation
10:30– 11:00	**Networking Break and Exhibits**
11:00– 12:30	**Panel Discussion: Measuring the Success of Insider Threat Programs** Senior Leaders recognize that insider threat poses significant and costly risks to national security. However, without clearly defined metrics, it may be difficult to see the precise return of investment in these programs, leading to insufficient resources, funding and missed opportunities for improvement. The panel will attempt to understand how success should be measured in insider threat detection and deterrence programs. Additionally, panelists will discuss the challenges of communicating the ROI of insider threat programs to senior decision makers in order to ensure programs are correctly managed. Moderator: **Mary O'Loughlin,** Senior Policy Analyst**,** National Insider Threat Task Force, FBI Detailee **(Confirmed)** Panelists: - **Mark Kelton,** Senior Vice President, National Security Solutions, DynCorp Int. **(Confirmed)** - **Sabeena Khanna,** Insider Threat Program Director, Department of Energy **(Confirmed)** - **David Denning,** Counterintelligence/Insider Threat Program Senior Manager, Northrop Grumman **(Confirmed)**

12:30 – 1:30	**Networking Lunch & Exhibits**
1:30 – 3:00	**Panel Discussion: Leveraging Artificial Intelligence in Modernized Insider Threat Programs** As technology becomes more complex, organizations have developed a need for a new approach to identifying accidental and malignant employee insider threat incidents with more accuracy and less guesswork. Artificial intelligence may offer organizations the ability to detect these potential risk patterns more quickly without the inherent bias of human observers. However, AI is no cure-all. Panelists from academia, industry and the government will discuss what they believe the role is for AI within their organization's insider threat enterprise. The panel will also touch on the potential drawbacks of AI technologies and areas where AI may fail to accurately detect insider threat behavior. Moderator: **Damon Woodard, Ph.D,** Associate Professor, Electrical and Computer Engineering Department, University of Florida **(Confirmed)** Panelists: - **Gordon B. Johnson,** Deputy Director, Counterintelligence Operations and Investigations, Lockheed Martin **(Confirmed)** - **Dan Costa,** Deputy Director, CERT National Insider Threat Center **(Confirmed)** - **John Sipple,** Expert in Applied AI**,** Senior Software Engineer in Machine Learning, Google; Joint Reserve Lead for AI Portfolio, Defense Innovation Unit **(Confirmed)**
3:00 – 3:30	**Networking Break & Exhibits**
3:30 – 4:15	**DHS's Approach to Safeguarding Classified Information from Insider Threats** - Guiding department-wide insider threat and identity management strategies - Leveraging advanced technologies to increase the security of classified networks and data - Maturing DHS's insider threat program to ensure it is effective in the modern threat environment **Richard McComb (Confirmed)** Chief Security Officer, Department of Homeland Security
4:15 – 5:00	**Minimizing Unauthorized Access to Information Through Robust User Activity Monitoring Policies** - Understanding overarching UAM policies - Examining the technical requirements of UAM solutions - Ensuring Agency UAM programs include the following capabilities: keystroke monitoring full application content, screen capture, file shadowing for all lawful purposes and attributable data **Robert Lerner (Confirmed)** Technical Director, National Insider Threat Task Force
5:00	**End of Day One**

October 24, 2019	
8:15 – 8:45	***Registration and Light Breakfast Reception Open***
8:45 – 9:00	**Chairperson Opening Remarks** **Moderator:** **Jim Onusko,** Director Strategic Solutions, LexisNexis Special Services **(Confirmed)**
9:00 – 9:45	**Establishing Operational Insider Threat Programs Across the DoD** - Furthering DoD InT efforts through UAM, behavioral analysis, data sharing, training and DITMAC - Overcoming challenges of data sharing across industry and DoD components - Adapting InT programs to changing technological and cultural variables and threat patterns **Dr. Brad Millick (Confirmed)** Director, Insider Threat Program, Office of the Under Secretary of Defense for Intelligence
9:45 – 10:30	**Safeguarding the Integrity and Trustworthiness of the Federal Workforce** - Transforming the background investigation enterprise to more efficiently leverage new technologies and continuous evaluation strategies - Understanding the changes to NBIB due to re-alignment under the DoD umbrella - Guiding the newly formed DCSA in continuous vetting and insider threat operations **Charlie Phalen Jr. (Confirmed)** Director, Defense Counterintelligence and Security Agency Director, National Background Investigations Bureau
10:30 – 11:00	*Industry Perspective with Securonix* **Beyond the Perimeter, Automating Finding Internal Threats** - Going beyond SIEM - Integrating behavioral analytics and SOAR. - Examining use case and threat models that work **David Swift (Confirmed)** Principal Architect, Securonix
11:00 – 11:30	**Networking Break & Exhibits**
11:30 – 12:45	**Panel Discussion: Reviewing the Success of the NITTF Insider Threat Program Maturity Framework** In November 2018, the National Insider Threat Task Force released the "Insider Threat Program Maturity Framework." The framework provides agencies with the minimum elements necessary to establish functional ItN programs. It is designed to help agencies become more proactive, comprehensive, and better postured to deter, detect, and mitigate insider threat risk. This panel will review the success of the framework one year after its release. Panelists will share their insights into, and lessons learned about, the various elements of the framework. **Moderator: David Buckley,** Managing Director, Risk Strategy and Compliance, KPMG **(Confirmed)**

	Panelists: - **COL Michael Birmingham, USA,** Division Chief, Insider Threat Division, US Army **(Confirmed)** - **J.T. Mendoza,** Deputy Director, USAF Insider Threat Hub **(Confirmed)** - **Lillian Samadani,** Assessment Team Lead, National Insider Threat Task Force **(Confirmed)** - **Joel Brush,** US Navy Insider Threat Hub **(Confirmed)**
12:45 – 1:45	**Networking Lunch**
1:45 –2:30	**Guiding US Navy Insider Threat and Counterintelligence Strategies** - Leading US Navy intelligence efforts - Mitigating current InTP inefficiencies due to information sharing and organizational gaps and seams - Leveraging sophisticated technologies to bolster insider threat detection - Expanding Insider Threat resources and working to create a physical InT Hub by FY2020 **Dr. Mark Livingston, SES (Confirmed)** Senior Director of Intelligence Deputy Under Secretary of the Navy for Policy
2:30 – 3:15	**Formulating Policies and Procedures for Mitigating the Loss of Classified Information** - Taking a multi-pronged approach to mitigating insider threat by balancing the use of cyber security technology, monitoring and human analysts - Ensuring the physical security of classified and sensitive documents - Implementing targeted employee training to improve security **Neil Carmichael (Confirmed)** Director, Insider Threat Program, National Archives and Records Administration
3:15 – 4:00	**The Psychology of Insider Threats: Leveraging Behavioral Science to Mitigate Threats** - Identifying malicious insiders by observing patterns of cyber-behavior - Understanding malicious information seeking behavior characteristics in order to successfully develop techniques for insider threat detection - Examining frontline employee identification of organization insider threat vulnerabilities **Dr. Deanna Caputo (Confirmed)** Chief Scientist for Behavioral Sciences and Cyber Security, MITRE
3:15	**End of Symposium**