Seminar Overview

Title: Knowledge Transfer within Industrial Security
Presenter: Michael Perez, Northrop Grumman

Abstract: Knowledge Management has been associated with Baby Boomer departures. However, this presentation offers security professionals new opportunities to leverage knowledge transfer to ensure organizations are equipped to move forward when personnel depart their organizations. Michael will provide an overview and examples of Knowledge Management implementation within Boeing and Northrop Grumman Security organizations. The topics covered will include the following: Knowledge Management, Knowledge Transfer (Tacit/Explicit), Knowledge Retention, and Barriers to Sharing Knowledge.

Title: They Know Us: OPM Data Breach: What is the Adversary Likely to Do with the Clearance Records for 20 Million Americans?
Presenter: Sina Beaghley, Rand Corp.

Abstract: Over the last decade, hackers have become increasingly sophisticated and brazen in their assaults on the systems that safeguard America's data. Amid a sea of highly concerning breaches, perhaps one of the most distressing is the recent breach on the Office of Personnel Management (OPM) background investigation information of over 20 million Americans. The full consequences of this hack raise a number of vexing questions. What are the repercussions that lurk in the US government's future? And what can a state-actor do with the background investigation records for the custodians of America's secrets? This presentation considers the possible and likely uses for the data by the adversary, and discusses some actions that victims can take to protect themselves.

Title: DFARS/CUI Update
Presenter: Jeff Bauer, ViaSat Compliance Mgr.

Abstract: The DoD mandate to implement the NIST 800-171 security controls no later than 31 December, 2017, for all federal contractors that process, store, or transmit Covered Defense Information (CDI) or provide "operationally critical support" in performance of a contract has resulted in a number of near-term and long-term challenges for small, medium, and large organizations alike. However, the NIST 800-171 security framework is only one variable of a three-pronged approach as a result of Defense Federal Acquisition Regulation Supplement (DFARS) Clause 252.204-7012; which in addition to NIST 800-171, federal contractors must also abide by cyber incident reporting requirements and address/validate the use of external Cloud Service Providers (CSP) in order to provide "adequate security" for the DoD's unclassified information that resides on a federal contractor's information system. Jeff Bauer will provide an overview of DFARS Clause 252.204-7012 and NIST 800-171 and how this will impact federal contractors in the near-term and long-term via a "Who/What/When/Where/Why/How" approach for the presentation with a focus on what will happen after 31 December, 2017.

Title: Defense Office of Hearings and Appeals (DOHA) Adjudication Process: *An Interactive Discussion on Recent Trends in Security Clearance Decisions*
Presenter: Brian Cruz, Counsel, Pillsbury Winthrop Shaw Pittman LLP

Abstract: We all know that receiving the dreaded yellow envelope from DOHA can be an overwhelming experience and the process can be daunting for our employees. Brian Cruz, Counsel with Los Angeles Law Firm Pillsbury Winthrop Shaw LLP will walk us through the adjudication process and lead a dynamic discussion on recent trends in the Security Clearance Process Decision.

Title: Privacy and the "Going Dark" Problem: Challenges to Surveilling and Countering Extremism
Presenter: Sina Beaghley, Rand Corp.

Abstract: In the wake of the terrorist attacks on September 11, 2001, the Patriot Act expanded U.S. government's authorities to surveil suspected terrorists in order to prevent future attacks. In the 15 years since, the US government has used those intelligence collection authorities to detect terrorist plotting and disrupt attacks. However, following the Edward Snowden unauthorized disclosures in 2013-2014, significant privacy questions were raised in the United States and around the world about the extent of such government surveillance activities. Privacy advocates and some in the technology sector have called to increase security of communications technology to better protect the privacy of individuals. However, there is the concern that such encryption measures could result in terrorists' communications "going dark" and the loss of critical insight into terrorist plotting to prevent an attack. So how should the government and citizens negotiate the desire for privacy with the need for security and public safety? What is the right balance? And what role should the commercial sector – especially the technology sector – play in all of this moving forward? This presentation seeks to provide historical context to this debate, explore the position of each side, and highlight the challenges that lie ahead in balancing activities to counter extremism with measures to protect privacy.