2017 Public-Private Analytic Exchange Program *Project Abstracts*

The 2017 Project Abstracts provide a brief overview of each topic team's research activities and final deliverables. Please reach out to the Department of Homeland Security Office of Intelligence and Analysis at AEP@hq.dhs.gov if you are interested in receiving a copy of any team's deliverable product.

Aviation Insider Threat

Protecting the Aviation Industry against the threat from insiders is everyone's responsibility. As we have seen through a multitude of past cases, insiders will continue to seek to challenge security countermeasures, exploit potential vulnerabilities, and increase their knowledge of security procedures for nefarious purposes.

Through a combined effort, this Aviation Insider Threat Working Group seeks to leverage the best practices of the Private Sector and Federal Government in efforts to establish a baseline standard in identifying and reporting insider threat. This standard will look to achieve consistent insider threat mitigation and awareness messaging to employees within the aviation ecosystem and perhaps the traveling public.

Future of Ransomware and Social Engineering

Extortion has long been a tool used to exploit information, behavior, and money out of its targeted victims. With an increase in the amount of available and advanced technology by nefarious actors, it should be expected that this has led to the development and sophistication of cyber extortion. Nefarious actors have used these technological advances to create malicious programs and deliver it to its targets via social engineering. A social engineering attack is often an orchestrated campaign against either numerous targets or one high valued target using a variety of digital, in-person or over the phone techniques. The ultimate goal of this attack to install malicious programs that steal intellectual property, credentials or money; after all, it is much easier to hack a human than an organization. This document will address the emergence of ransomware, the maturation process of the malware, and examine the how social engineering is used in support of ransomware attacks; examine some of the potential future scenarios affecting how and why adversaries will utilize of ransomware; while also focusing on non-financial motivating factors that could advance, promote, or advertise nation-state or political causes.

Going Dark: Impact to Intelligence and Mitigations

The public and private sectors face a growing national security concern resulting from the ability of criminals, terrorists and state actors to obfuscate their activities by 'going dark' through encryption or other means. Rapidly evolving technological advancements—particularly in digital and communications security—impede the ability of US law enforcement and intelligence agencies to collect and analyze information critical to thwarting potential threats. This paper aims to explore the opportunities and challenges for law enforcement and the IC posed by the going dark problem. The paper will provide recommendations and next steps to update domestic and foreign policies, improve law enforcement tactics and examine solutions to overcome threat intelligence analysis and collection tactics hampered by encryption. The overarching goal is to promote private and public sector collaboration to help mitigate potential going dark threats and to further the policy debate.

Identifying and Mitigating Supply Chain Risks Posed by SCADA Systems in the Electricity Sector

This team will build on last year's AEP Energy Sector supply chain project by continuing to research threats posed to the electricity delivery sector via its supply chain. They researched threats posed by foreign adversaries - and possible avenues of exploitation of equipment - in the electricity delivery sector. The focus Supervisory Control and Data Acquisition (SCADA) systems which are computer systems for gathering and analyzing real time data as well as monitoring and managing industrial control systems embedded within the transmission and distribution portions of the electric grid. This research provided the best practices used by companies to mitigate risks to SCADA systems.

Intellectual Property Rights: Risks and Opportunities Throughout the Innovation and Product Life Cycle

Intellectual property (IP) theft has long threatened the success of innovators, industry, and the state. This threat has been amplified in the interconnected and global ecosystem of the 21st century digital economy, where emerging technologies have made possible new and more effective methods for exploiting the efforts of innovators. Theft of IP also poses a significant and growing threat to consumer health, safety, and trust, as well as adversely affecting the U.S. economy and national security. This paper explores the risks and opportunities associated with intellectual property rights throughout the innovation and product life cycle. We identify how the illicit use of technology, such as cloud computing, the internet of things, and 3D printing, can simplify IP theft, enable illegal entry into the marketplace, and streamline product

delivery. We also consider proactive measures IP owners can take to mitigate the risks to their intellectual property and also create opportunities for increased company value.

Likely Strategies that Influence Resilient Communities

The primary objective of this teams was to increase community resilience. Communities become more resilient to various hazards by adopting strategies and conducting activities in advance of, and in response to, specific catastrophic events. While it is difficult to extrapolate consistent strategies across different hazards and communities, the team explored the tools or methodologies communities use for assessing imminent or actual threats or damage; raising awareness on threats, behaviors, indicators; increasing vigilance; and encouraging preparedness. The team developed a high-level point of view to assess whether or not they are actually effective and/or impactful.

This was accomplished and developed high-level metrics for assessing the effectiveness of our communications and whether or not the communications increases community resilience; looked to identify changes in behavior (e.g., increased registration with regional automated notification services, increased attendance at community meetings, social media analysis indicating consumption of and identification with our messages, messages being relayed by community leaders, etc.); and looked at the communities in a more detailed way to understand the impact of communications. Are there specific key communicators, trusted organizations, lines of persuasion, or symbols that resonate more than others within the various groups? Are there vulnerable populations we may want to seek out and communicate with in a very specific way (e.g., elderly, recent immigrants, younger children, etc.)?

Opportunities and Risks of Contactless Biometrics

In recent years, we have seen great progress in contactless biometrics for entities requiring accurate and expeditious proof of identity. In this whitepaper, we address the state of the art technology and techniques used in recognizing individuals using contactless biometrics such as face, iris and voice recognition for the purposes of identification, investigation and authentication of individuals. We examine the limitations and challenges; and identify the obstacles that must be overcome in order for this technology to reach its full promise. In particular, we examine ways in which law enforcement agencies and private sector companies can leverage these new forms of PII without encroaching on civil liberties or compromising intellectual property. We conclude with recommendations for the path forward in public/private collaboration in this area.

Risks and Vulnerabilities of Virtual Currency

Virtual currency is a digital asset that enables monetary value exchange worldwide. This research focuses on cryptocurrencies (like Bitcoin), which are virtual currencies that rely on cryptography to produce assets and validate transactions. The emergence of virtual currencies and their associated technologies provide new methods of payment and have broad implications for illicit actor groups, consumers, official sector entities, and financial institutions. This paper will examined the positive and negative attributes and characteristics of common cryptocurrencies as they pertain to illicit actor groups, consumers, official sector entities, and financial institutions. This research explores the risks and challenges facing each group in using cryptocurrencies as a payment method. The findings provide strategic decision makers of commercial and government entities a framework to conceptualize and understand virtual currency attributes and their characteristics which may entail risks, or drive or inhibit adoption.

Technology and Automobiles Implications and Risks

Members of the U.S. Intelligence Community (USIC) and Private Sector propose this paper that discusses the technological implications and risks facing the automotive industry as well as any public or private organizations that may use the technology in the future. The group focused on identifying a standard model that aids in mitigating specific threats into categories. These categories focus on specific areas where technical components are at risk for intrusion; wireless connectivity, malware, vehicle control systems, sensors, and physical connections. Using this approach, the group attempted to develop a uniform risk assessment framework to measure the different types of exposures that connected vehicles pose to the both the private sector and the U.S. Government. In order to develop this framework the group conducted research on approved risk models highly rated and used by technology industries. The group also sought out to conduct interviews with several autonomous vehicle industry experts to gain insight on the various methods and techniques utilized against potential compromising attacks. As a result of collaborative research, interviews and subject matter expert input, the team developed a standard framework that the automotive industry and U.S. government could implement. The framework would return specific levels that would determine the level of vulnerability that the sector of the autonomous vehicle could face. The group implemented the Key Intelligence Questions (KIQs) and utilized the National Highway Traffic Safety Administration (NHTSA) guidelines on safety related defects and automated safety technology as a baseline guide for best practices

Threats to Undersea Communications

Carrying 97% of all intercontinental communications in 2015, privately-held commercial undersea communications cables are critical to international trade and commerce. Despite protection measures, undersea cables are susceptible to disruption to internet and other communications by physical threats, both accidental and malicious. This paper is a joint analytical product of interest for the primary target audience of the executive leadership of private and public users of undersea cable services. The intent is to inform senior management of potential risks from degraded or interrupted services, risk-mitigations currently in place, as well as business continuity options. Additionally, focus is also given to undersea cable operators and telecommunication firms with recommendations for improving physical security risks commonly seen at cable landing points and stations, as well as cable laying ships.

Unmanned Aircraft Systems Futures

As the integration of unmanned aircraft systems into the national airspace system for legitimate commercial purposes moves forward, reports of UAS encounters across multiple critical infrastructure sectors will continue to challenge the ability to characterize benign, suspicions or malicious intent. This team examined development of UAS out to 2020, for legitimate applications, and explore areas which offer the potential for crossover to malicious use. In addition to a set timeframe, the Subcommittee imposed criteria to scope the problem set. These criteria were meant to identify the area of largest market growth over the next ten years, according to a Federal Aviation Administration study.

The team identified the integration of UAS into security operations, as an avenue an additional identifying future use of UAS capabilities and security concepts. As part of an AEP funded research program, we organized, designed and conducted a two-day seminar, hosted by the Department of Homeland Security, National Urban Security Training Laboratory in New York City, examining the security integration requirements for future UAS operations. In preparing for this seminar, we sought out organizations that are using UAS in their operations, as well as security managers and private sector partners to identify future planning requirements, and help inform future information needs.