



## 2019 Public-Private Analytic Exchange Program (AEP) Topics

---

**Best Practices in Vetting Prospective and Current Employees:** This topic will examine how government and private sector can partner to share information on screening procedures for prospective and current employees. Additionally, this topic could explore legal and technological challenges, best practices with evaluating insider threats, and potential recommendations to make processes more effective and efficient.

**Combatting Targeted Disinformation Campaigns:** This topic will explore options to combat targeted disinformation campaigns by criminal and nation state actors. Additionally, this topic could also explore potential tactics, potential impacts to brand reputation, the use of emerging “deep-fake” technology and “big-data” in influence operations, and ways in which U.S. entities (both public and private) could detect, deter, and respond to these campaigns.

**Counterterrorism Futures:** This topic will explore how government and private sectors can partner to better secure the U.S. from terrorist attacks in light of shrinking government counterterrorism funding. Additionally, this topic could delve into how to optimize current public-private partnerships and explore potential technological solutions and legal challenges or opportunities to these types of partnerships.

**E-Commerce: Illicit Actors' Use of Reshipping Services:** This topic will explore how illicit actors are exploiting their access to millions of commercial goods via online electronic commerce (e-commerce) platforms in the U.S., as well as the use of reshipping services to obfuscate the final destination. Additionally, this topic could explore challenges to both the private and public sectors to detect, mitigate, and deter sub-standard or illicit trade; and identify opportunities for international collaboration, current trends, and potential mitigation strategies.

**Geopolitical Impact on Cyber Threats from Nation-State Actors:** This topic will explore the impact of geopolitical events on the cyber threat from Russia, China, Iran, and North Korea that influence operations. Additionally, this topic could also address possible targets of state-sponsored cyber-attacks, lessons learned from recent incidents, and potential mitigation strategies to prepare for future threats.

**Identifying Risks to Vehicle Technology Advancements:** This topic will address the potential for cyber actors to exploit current and emerging technology in vehicles. This topic could also delve into supply chain risks from counterfeit vehicle technology components, government use of data stored on vehicles, and the potential introduction of vulnerabilities from third party accessories. The topic will also discuss potential considerations for manufacturers, regulators, and consumers to address or mitigate these risks.

**Industrial Internet of Things (IIOT) Interconnections:** This topic will explore the possible vulnerabilities and risks associated with the implementation of IIOT devices on industrial control systems (ICS) and supervisory control and data acquisition (SCADA) networks. Additionally, this topic will also address approaches to mitigate potential security vulnerabilities, interdependencies across critical infrastructure sectors, and how the government and private sector stakeholders can work together to mitigate risks.

**Strategies to Address Physical Supply Chain Risks:** This topic will explore potential risk management technologies or methodologies that could enhance the integrity of U.S. supply chain efforts. Additionally, this topic could address current challenges and vulnerabilities impacting global trade flows, legal constraints and opportunities, and potential strategies which can be jointly employed by the government and private sector stakeholders.