2021 PUBLIC-PRIVATE ANALYTIC EXCHANGE PROGRAM

## 2021 Program Topics

**Emerging Threats to Cargo and Port Security:** This topic will explore emerging threats to cargo and port security from increasingly sophisticated hostile actors as well as the potential damage to economic, security, and commercial interests. This topic could focus on new threats such as cyber intrusions and unmanned underwater vehicles and examine how government and private companies may jointly address these mutual threats.

**Evolving Cyber Legal Landscape:** This topic will explore the risk and implications of current and future data regulations that cross international boundaries for U.S. entities. This topic could address the impact or current and proposed legislation on the collection, storage, and transmission of data as well as the potential vulnerabilities to information technology architecture located in foreign countries.

**Importance of Private Sector Intelligence Programs:** This topic will examine the important role of private sector intelligence programs in an increasingly dynamic threat environment and how government and private companies could partner in ways to bolster these programs to address mutual threats. This topic could focus on sharing best practices and lessons learned in areas such as analytic tradecraft, personnel training, and organizational structure.

**Improving U.S. Competitiveness in the Global Market:** This topic will examine the growing threat from foreign countries and their state-backed companies to U.S. competitiveness and influence on the world stage. It will also explore how the U.S. Government and private U.S. companies could work more closely to improve American competitiveness in the global market. This topic could focus on China's Belt and Road Initiative (BRI) as a case study, in which Beijing is using this program to expand into new markets and build its influence across the region.

**Increasing Threats of Deepfake Identities:** This topic will explore emerging technological threats to identity information, such as user impersonation, and examine ways in which government and private companies could partner to better detect, mitigate, and prevent these threats. This topic could focus on identifying deepfakes and other forms of disinformation that endanger both the public and private sector.

**Privacy and Security Implications of 5G Technology:** The topic will examine new privacy and security implications associated with 5G technology, which will radically improve the bandwidth, capacity, and reliability of mobile broadband. This topic could focus on opportunities for government and private companies to partner to address new threats and vulnerabilities as 5G technology becomes more widely available.

**Protecting Sensitive Data and Intellectual Property:** This topic will explore the increasing threat to sensitive data and IP as the theft of this information becomes more common and widespread. This topic could examine recent incidents of data and IP breaches across both the public and private sector to better enable organizations to identify targets and protect sensitive information from internal and external actors.

**Threats to U.S. Food and Agriculture Sources:** This topic will examine threats to food sources that could disrupt, destroy, or deny accessibility of food in the U.S. or impact agricultural trade. This topic could explore the intentions and capabilities of hostile actors as well as their tactics, techniques, and procedures to target food sources.

**Phase Teams:** Originating prior to AEP 2020, these topic teams identified area of their topic to further investigate and requested a continuation for "Phase 2 or 3". Here is a list of Phase 2 and Phase 3 Topic Teams of AEP 2021:

- **Phase 2**: **AEP 2019 Best Practices in Vetting Prospective**
- **Phase 2: AEP 2019 Current Employees and Combatting Disinformation Campaigns**
- **Phase 3: AEP 2018 Vulnerablitites of Healthcare Information Technology Systems**