Panel

- **Tonya Ugoretz**, Director, Cyber Threat Intelligence Integration Center, ODNI
- **Scott DePasquale**, President and CEO, Financial Systemic Analysis and Resilience Center
- **Bob Kolasky**, Director, National Risk Management Center, DHS
- **Jared Maples**, Director, New Jersey Office of Homeland Security and Preparedness
- **Joe Nimmich**, Senior Executive Advisor, Booz Allen Hamilton (moderator)

Topic Overview

Essential services across a variety of sectors – including energy, transportation, shipping, and communications – are all vulnerable to attacks from foreign states, non-state actors, and rogue elements, with wide-ranging ramifications for public safety, commerce, and national security. Public-private collaboration and information sharing – particularly through state intelligence fusion centers, information sharing and analysis centers (ISACs), and DHS's new National Risk Management Center (NMRC) – can help private companies prioritize their risk management initiatives.

Panel Summary

Panelists discussed how stakeholders should share information; the mission of DHS's new National Risk Management Center; threats to, and vulnerabilities of, the financial sector; and the importance of information-sharing to promote critical infrastructure resilience.

Panelists stated that stakeholders should share information through established mechanisms such as state intelligence fusion centers and government-industry partnerships, such as sector-specific ISACs. These centers enable federal, state, local, and private sector entities to share information about critical infrastructure resilience. The NMRC, whose mission is to provide a centralized home for collaborative, sector-specific and cross-sector risk management efforts to better protect critical infrastructure, is another potential collaboration and information-sharing mechanism.

The financial sector is particularly vulnerable to cyber threats such as social engineering attacks, mobile threats, and data breaches. Social engineering and phishing, which represent some of the simplest and most profitable attacks, have profited from the widespread use of online and mobile banking by technologically unsophisticated consumers. A resilient critical infrastructure system will require continued information-sharing between federal, state, and local governments and their industry partners.
Key Insights:

- DHS’s new National Risk Management Center will conduct planning and analysis to help industry prioritize risk management efforts.
- Existing public-private coordinating mechanisms – such as state intelligence fusion centers and sector-specific information sharing and analysis centers – should be used to share information and coordinate decision making by government and industry.
- Thanks to geography, cyber incidents often have cascading effects; an attack on infrastructure in New York City, for example, will have spillover effects on infrastructure and populations in New Jersey.

Recommendations:

- Continue and expand public-private collaboration to improve resiliency and response to cyber attacks.
- Formalize cyber incident response roles of information-sharing mechanisms, such as ISACs, to ensure transparency during a crisis.
- Provide incentives for government and industry to share all relevant information in a crisis without fear of political or financial repercussions.
- Conduct public-private training and exercises, such as the tabletop exercise (TTX) conducted by INSA, to identify key vulnerabilities in critical infrastructure resilience and cyber incident response.
- Encourage infrastructure operators and other private companies to work closely with DHS’s National Risk Management Center to prioritize risk management efforts.

Thank You, Sponsors and Partners:

ABOUT INSA
The Intelligence and National Security Alliance’s mission is to foster dialogue between public and private elements of the national security sector. INSA approaches this mission through a variety of means, including by organizing conferences, symposia, exercises, and other discussions. INSA also convenes government and industry experts in nine policy councils that address topics ranging from security clearance reform and insider threats to acquisition management and intelligence law.