DHS Officials Push for Cyber Information Sharing

In late February, two Department of Homeland Security (DHS) officials testified before a congressional panel on President Obama's proposal on cybersecurity information sharing.

Under Secretary Suzanne Spaulding and Deputy Under Secretary for Cybersecurity & Communications Phyllis Schneck addressed the House Committee on Homeland Security, highlighting the National Protection and Programs Directorate cybersecurity role and capabilities, and speaking of DHS's plans to facilitate better information sharing of cyber threats between private industry and the federal government through the National Cybersecurity and Communications Integration Center (NCCIC).

Spaulding and Schneck described NCCIC's relationship with its partners – which include both private sector organizations and federal departments and agencies, among others – and NCCIC's work sharing cyber threat indicators with these partners.

The officials discussed President Obama's recent visit to NCCIC, where he announced new cybersecurity legislation to better facilitate information sharing between the government and the private sector. According to Spaulding and Schneck, "Our vision is that this may reduce the time to receive and act on indicators from hours to milliseconds, create consistency in information provided to interagency partners, law enforcement, and the private sector".

Spaulding and Schneck also reviewed new developments in DHS's cyber threat information sharing efforts, including specifications which standardize the representation and exchange of cyber threat information. ***IAJ***

Cybersecurity, Consumer Protection Subject of White House Summit

Stanford University hosted the White House Summit on Cybersecurity and Consumer Protection on February 13. The summit centered around cybersecurity information sharing and the efforts private industry is taking to better protect the data of their customers. The event brought together leaders from various industries, law enforcement, consumer and privacy advocates, academics, and students.

Lisa Monaco, homeland security and counterterrorism advisor to the President, opened the summit. Monaco, who recently announced the creation of the Cyber Threat Intelligence Integration Center (CTIIC), spoke of the growing importance of cybersecurity issues related to national and homeland security, including in the financial, energy, and technology sectors. Monaco also spoke about the continuing rise in cybersecurity breeches and attacks, the effort needed to meet a "constantly evolving enemy," and the value of private sector cooperation with the government to address cyber threats.

The summit included several plenary panels, the first of which dealt with public-private collaboration on cybersecurity. Panelists included CEOs from consumer retail, banking, health care, and utility companies, and the panel was moderated by Secretary of Homeland Security Jeh Johnson. In his remarks, Kenneth Chenault, Chairman and CEO of American Express, described the cyber threats faced by the U.S. as "increasingly challenging, increasingly complex" and went on to say that "information sharing may be the single, highest impact, lowest cost, and fastest way

to implement capabilities we have at hand as a nation to accelerate our overall defense from the many varied and increasing threats that we are facing every second."

President Obama made the keynote address, centering his remarks on confronting cyber threats and the future of cybersecurity. During his address, the President also introduced and signed an executive order encouraging the sharing of cybersecurity threat information within the private sector and between the private sector and government.

Later panels focused on consumer data protection, and featured panelists from various industries, including credit card companies and large businesses. ***IAJ***

Executive Order Calls for Information Sharing of Cyber Threat Data

On February 13, President Obama signed an Executive Order to encourage and promote sharing of cybersecurity threat information within the private sector and between the private sector and government. The Executive Order lays out a framework for expanded information sharing designed to help companies work together, and work with the federal government, to quickly identify and protect against cyber threats.

The Executive Order encourages private sector cybersecurity collaboration through information sharing and analysis organizations (ISAOs), and directs the Department of Homeland Security to fund the creation of a non-profit organization to develop a common set of voluntary standards for these ISAOs. The Executive Order also increases collaboration between ISAOs and the federal government, and will streamline private sector companies' ability to access classified cybersecurity threat information.

The new Executive Order complements the Administration's January 2015 legislative proposal, and paves the way for new legislation, by building out the concept of ISAOs as a framework for the targeted liability protections that the Administration has long asserted are pivotal to incentivizing and expanding information sharing. ***IAJ***

New Agency to Investigate Cyber Threats

In February, the White House announced that it is creating a new office analyze and integrate intelligence data about cyber threats and combat cyber attacks. The Cyber Threat Intelligence Integration Center (CTIIC) will fall under the purview of the Office of the Director of National Intelligence.

Lisa Monaco, assistant to the President for homeland security and counterterrorism, introduced the CTIIC during a talk at the Wilson Center, saying that "What we need is critical, rapid, integrated intelligence."

The CTIIC will be modeled after the National Counterterrorism Center (NCTC), and will integrate intelligence from the Central Intelligence Agency, National Security Agency, and other federal agencies, as well as the private sector. The CTIIC will focus on four priorities:

- Improving cyber defense, including widespread adoption of the NIST Cybersecurity Framework;