

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;

- Improving the ability to disrupt, respond to and recover from attacks;
- Enhancing international cooperation; and
- Making cyberspace intrinsically more secure, including eliminating passwords as the default security tool and enhancing consumer protection.

In her remarks, Monaco stated that “Cybersecurity is and will remain a defining challenge of the 21st century,” and that “The choices we make today will define the threats we face tomorrow. **IAJ**

White House Discusses Strengthening U.S. Cybersecurity

On January 14, President Obama visited the National Cybersecurity and Communications Integration Center (NCCIC) where he spoke about plans to strengthen U.S. cybersecurity in 2015. His remarks at NCCIC come a week before his State of the Union address.

During his address at NCCIC, the President announced new cybersecurity legislation to better facilitate information sharing between the government and the private sector. This legislation improves upon prior legislation, builds on discussions with the federal government and private industry, and includes safeguards to protect Americans’ privacy and civil liberties.

The new cyber efforts also include updating the authorities used by law enforcement when investigating and prosecuting cyber criminals. This would include prosecuting those involved in the sale of botnets and spyware, and expands the authority of courts to shut down botnets and other malware.

The President also announced that a White House Summit on cybersecurity and consumer protection would be held in February at Stanford University. The summit will include participants from the U.S. government and across various industries, technology companies, and consumer and privacy advocates, as well as law professors and students.

President Obama concluded his remarks saying that the U.S. government and private sector would work together to “detect, prevent, defend, and deter” cyber attacks. **IAJ**