Cybersecurity Bill Passes Senate Intelligence Committee

On March 13, the Senate Select Committee on Intelligence voted the Cybersecurity Information Sharing Act of 2015 through by 14 to 1. The bill will now move on to the Senate.

The Cybersecurity Information Sharing Act of 2015 creates additional incentives to increase voluntary sharing of cybersecurity threat information between the private sector and the federal government while protecting individual privacy and civil liberties interests. The bill also offers liability protection to the private sector.

The bill tasks the Department of Homeland Security with setting up a mechanism to receive threat indicators from network operators, and includes plans for government to share classified and other non-public threat information with "cleared representatives of relevant entities."

The Cybersecurity Information Sharing Act of 2015 was co-sponsored by Committee Chairman Richard Burr (R-NC) and Vice Chairman Dianne Feinstein (D-CA). ***IAJ***

Air Force Restructures Nuclear Weapons Center

The Air Force Nuclear Weapons Center was recently restructured to better serve the Nuclear Enterprise. On March 30, the center added two new directorates, including the Nuclear Technology and Interagency Directorate.

The new Nuclear Technology and Interagency Directorate focuses on nuclear weapons technology and interagency cooperation and partnership in the nation's nuclear enterprise. The Nuclear Technology and Interagency Directorate enhances the Air Force Nuclear Weapons Center support of the U.S. nuclear deterrence and assurance responsibility, and ensures this mission is carried out through the acquisition, sustainment, and support of powerful weapon systems.

Air Force Nuclear Weapons Center commander Maj. Gen. Sandra Finan spoke of the center's reorganization, saying "Our mission is still to deliver nuclear capabilities and winning solutions that warfighters use daily to deter our enemies and assure our allies. Implementation of this [structure] will better align our organization to that mission." ***IAJ***

Interagency Strategy Needed on Drones

On March 18, members of the House Homeland Security Subcommittee on Oversight and Management called for better comprehensive strategy to combat the potential threats of domestic drones, sometimes referred to as unmanned aerial systems or unmanned aerial vehicles.

In his opening statement, Subcommittee Chairman Rep. Scott Perry (R-PA) expressed concerns about the potential for drones to be utilized by terrorists, drug smugglers, and spies, and cited recent security incidents, such as the quadcopter crash at the White House and drones flying over Parisian landmarks and nuclear power plants.

Several witnesses spoke about the need for interagency cooperation to address the drone issue in their statements to the Subcommittee.

Major General (Ret.) Frederick Roggero, United States Air Force, called for interagency cooperation to draft strategy and policies to deal with drones, saying that "it will take a joined effort across all government departments since it will require navigating through current rules and

regulations in the face of the unique capabilities of [drones]".

In his statement, Chief Richard Beary, President of the International Association of Chiefs of Police, cited a lack of instruction for law enforcement regarding the use of drones, and spoke of the need for greater tactical guidance to law enforcement from federal agencies, including the Departments of Homeland Security, Justice, Defense, and the Federal Aviation Administration. According to Beary, such guidance "would benefit the law enforcement profession immensely".

Dr. Gregory S. McNeal, Associate Professor at the School of Law at Pepperdine University, also expressed a need for greater interagency cooperation, suggesting that the Department of Homeland Security be responsible for coordinating interagency efforts, as opposed to the agencies working separately. McNeal also suggested the department engage in a comprehensive risk assessment. ***IAJ***

CSIS Report Provides Recommendations on Cyber Threat Information Sharing

In early March, the Center for Strategic & International Studies (CSIS) published a report outlining their recommendations to Congress in regard to cyber threat information sharing between the government and the private sector.

To identify lessons learned from existing and previous information sharing efforts, CSIS convened three workshops to discuss the technical, structural, and legal challenges to cyber threat information sharing. These workshops were attended by a cross-sector stakeholder group that included government, industry, and privacy organizations, as well as experts from the financial services, telecommunications, electricity, oil and gas, retail, and commercial information technology sectors, and the privacy community.

After analyzing the comments and suggestions of the participants, the authors have provided Congress with 11 recommendations for policy and legislation. These recommendations cover both structural and legal issues, and include:

- Private-to-private sharing with a minimal role for government can help promote voluntary information sharing and alleviate privacy concerns.
- Build upon existing information-sharing organizations and mechanisms.
- Cyber threat information shared voluntarily with the government should be protected from disclosure through Freedom of Information Act (FOIA) requests and barred from use in civil litigation or regulatory purposes.
- Identify ways for information sharing models to demonstrate value for all parties involved.
- Permissible law enforcement uses of cyber threat information shared by companies with the government should be restricted to cybersecurity purposes and a limited set of other activities.
- Legislation should authorize monitoring and sharing of cyber threat information, and provide a safe harbor from civil and criminal liability for good-faith actions in conducting such activities.

While the authors recognize that there is much to be gained through improved cyber threat information sharing, they also note that it is not "an end in itself," and suggest that the government and other sectors "articulate the objectives and goals for information sharing, and tailor mechanisms for information sharing to achieve those goals." ***IAJ***