Cooley

December 17, 2015

The **Omnibus appropriations bill** entitled the Fiscal Year 2016 Consolidated Appropriations Act released late Tuesday, includes language from separate cybersecurity bills that had previously passed in both the House of Representatives and Senate. This represents a somewhat historic event. After many years of wrangling over cybersecurity legislation, Congress finally has been able to craft information sharing language that has bipartisan appeal and, therefore, hasn't gotten rejected.

Specifically, the Senate passed the Cybersecurity Information Sharing (CISA) in October with a bipartisan 74 to 21 vote and the House of Representatives passed two cyber-related bills, the Protecting Cyber Networks Act (PCNA), and the National Cybersecurity Protection Advancement Act (NCPAA) in April with a similarly strong bipartisan votes of 307-116 and 355-63 respectively. Both CISA and PCNA provide companies with liability protections when sharing cyber threat data with government agencies in order to strengthen the United States' digital defense against cyberattacks. Since the October Senate vote, members of the House and Senate had been in talks to reconcile the bills to reach a compromise. Those conversations led to a workable compromise and the "must-pass" Omnibus appropriations bill provided a legislative vehicle to have the compromise version signed into law.

Division N of the Omnibus appropriations bill contains the Cybersecurity Act of 2015 – the new name for the combined CISA and PRNA/NCPAA bills. According to the authors of the legislation, the compromise bill "is designed to create a *voluntary* cybersecurity information sharing process that will encourage public and private sector entities to share cyber threat information, without legal barriers and the threat of unfounded litigation – while protecting private information."

The Cybersecurity Act of 2015 is divided into four titles. Title I, entitled Cybersecurity Information Sharing, outlines the definitions used in the act and establishes liability protections for companies that share cybersecurity threat information with the government. Title II, entitled National Cybersecurity Advancement, outlines steps to strengthen the government's existing cybersecurity response system and adds new directives for cybersecurity advancement going forward. Title III, the Federal Cybersecurity Workforce Assessment, outlines that an inventory of existing government workforce addressing cybersecurity issues shall be taken and reports should be made about necessary workforce deficiencies. Title IV, entitled Other Cyber Matters, details future actions that shall be taken to strengthen cybersecurity including, among other things, studies on mobile device security, enhancement of emergency services, and improving cybersecurity in the healthcare industry.

Title I of the Cybersecurity Act contains some of the most controversial and critical provisions intended to establish effective sharing of information between the private and public sector. Below are two key sections of Title I, with descriptions derived, in part, from the joint statement of the Senate Select Committee on Intelligence, the House Permanent Select Committee on Intelligence, the Senate Committee on Homeland Security and Governmental Affairs, and the House Committee on Homeland Security:

Section 105 – Sharing of cyber threat indicators and defensive measures with the Federal Government

Section 105 directs the Attorney General and Secretary of Homeland Security (the "Secretary") to jointly develop policies and procedures for governing the sharing of information by the Federal Government about cyber threats. As part of such development, Section 105 contemplates creation of an automated real-time process that allows for information systems to exchange identified cyber threat information without manual efforts, subject to limited exceptions that must be agreed upon in advance. Section 105

also directs the Attorney General and the Secretary, in coordination with heads of appropriate Federal entities and in consultation with both privacy officials and private entities, to jointly issue and make available final guidelines addressing privacy and civil liberties for Federal entity-based cyber information sharing.

Further, Section 105 directs the Secretary, in coordination with heads of appropriate Federal entities, to develop, implement, and certify the process by which the Federal Government may receive cyber threat information shared by a non-Federal entity. It also provides authority to the President to designate a Federal entity, other than the Department of Defense (including the National Security Agency), to develop and implement an additional capability and process following a certification and explanation to Congress. Section 105 clarifies that otherwise lawful disclosures of information related to criminal activities, Federal investigations, or statutorily or contractually required disclosures would not be prohibited. However, this section does not preclude the Department of Defense, including the National Security Agency from assisting in the development and implementation of a capability and process established consistent with this title. Further, any other department or agency will not be precluded by Section 105 from requesting technical assistance or staffing a request for technical assistance.

Section 105 further provides that cyber threat information shared with the Federal Government does not waive any applicable privilege or protection, may be deemed proprietary information by the originating entity, and is exempt from certain disclosure laws. Cyber threat information may be used by the Federal government for: cybersecurity purposes; identifying a cybersecurity threat or vulnerability; responding to, preventing, or mitigating a specific threat of death, a specific threat of serious bodily harm, or a specific threat of serious economic harm, including a terrorist act or a use of a weapon of mass destruction; responding to, investigating, prosecuting, preventing, or mitigating a serious threat to a minor; or preventing, investigating, disrupting, or prosecuting an offense arising out of certain cyber-related criminal activities.

Finally, Section 105 provides that cyber threat information shared with the Federal Government shall not be used by any Federal, State, tribal, or local government to regulate non-Federal entities' lawful activities.

Section 106 – Protection from liability

Section 106 provides liability protection for private entities that monitor, share, or receive cyber threat information in accordance with Title I, notwithstanding any other provision of Federal, State, local, or tribal law. Section 106 further clarifies that nothing in Title I creates a duty on any specific entity to share cyber threat information or a duty to warn or act based on receiving cyber threat information. At the same time, nothing in Title I broadens, narrows, or otherwise affects any existing duties that might be imposed by other law; Title I also does not limit any common law or statutory defenses.

In addition to the provisions of Section 105 and Section 106, the Cybersecurity Act of 2016 also contains important privacy and civil liberties protections. For example, Section 103 requires the Director of National Intelligence, the Secretary of Homeland Security, the Secretary of Defense, the Attorney General, and heads of certain Federal entities to jointly develop and issue procedures to operationalize the sharing of cyber threat information. Such procedures will require either (a) a review by a Federal entity of cyber threat indicators for, and removal of, any personal information or (b) a technical capability to remove personal information unrelated to a cybersecurity threat. Further, the procedures will require notification of any disclosure of personal information inconsistent with provisions of the Cybersecurity Act. Similarly, Section 107 contains a requirement for a report to be produced at the three-year mark that will evaluate the efficacy of the information removal procedures in Section 103.

The House and Senate likely will vote on the Consolidated Appropriations Act on Friday. Most commentators agree that passage is likely. It is expected that it will be signed into law by the President. Passage could affect a number of different entities that may be investigating the advantages, disadvantages, and associated liabilities of information sharing or actively considering how to work information sharing into their cyber portfolio. For questions on this, or any other bill having cyber components, please contact our **Privacy & Data Protection practice**.

Key Contacts

Randy Sabett Washington, DC	rsabett@cooley.com +1 202 728 7090
Vince Sampson Washington, DC	vsampson@cooley.com +1 202 728 7140