Privacy and Information Governance

# Key Provisions of Cybersecurity Act of 2015

By: Mary Ellen Callahan, Nancy C. Libin and Heidi L. Wachs

On December 18, 2015, Congress passed the Cybersecurity Act of 2015 as part of the Consolidated Appropriations Act. On December 16, Congress initially incorporated the information-sharing legislation as part of the proposed consolidated appropriations bill. The Act is the culmination of a conference committee that incorporated elements of three cybersecurity bills passed earlier this year.

Broadly, the Act provides a framework for non-federal entities and federal entities to share cybersecurity information with each other. Any such sharing by non-federal entities will be voluntary. Non-federal entities that share cybersecurity information with federal entities will receive certain antitrust and other liability protections. The Department of Homeland Security (DHS) will serve as the primary federal government recipient of the information through the DHS National Cybersecurity and Communications Integration Center.[1]

Key provisions of the Act include:

***Development of Cyber Threat Information Sharing Procedures***

The Act requires the Director of National Intelligence, the Secretary of Homeland Security, the Secretary of Defense, and the Attorney General to jointly develop and issue procedures for the timely sharing of cyber threat indicators (CTIs) and defensive measures (collectively, "cyber threat information"). Among other requirements, these procedures must:

- Ensure that the federal government has the capability for the real-time sharing of cyber threat information;
- Include a process for notifying entities that have erroneously received cyber threat information;
- Include procedures governing how federal entities, prior to sharing cyber threat information, will review and remove any information "not directly related to a cybersecurity threat" known at the time of sharing to be the personal information of a specific individual or information that identifies a specific individual or, alternatively, to implement a technical capability to do the same (*e.g.,* a "scrub").

***Antitrust Protection, Monitoring and Operating Defensive Measures***

Private entities will not violate antitrust laws when they share cyber threat information or assist each other with the prevention, investigation, or mitigation of a cybersecurity threat. Private entities are authorized to monitor their own information systems and operate defensive measures. They may also monitor the information systems of other non-federal or federal entities, and operate defensive measures on those information systems, if they obtain authorization and written consent.

***Cyber Threat Information Sharing Among federal Government Entities***

The Attorney General and the Secretary of Homeland Security are charged with jointly developing policies and procedures to govern sharing of information about cyber threats among entities in the federal government. The Act requires this sharing to be done through an automated real-time process, subject to limited exceptions that must be agreed upon in advance. In addition, the Attorney General and Secretary of Homeland Security, in consultation with the heads of appropriate federal entities and other designated officers, must jointly "develop, submit to Congress, and make available to the public…guidelines relating to privacy and civil liberties which shall govern the receipt, retention, use, and dissemination of cyber threat indicators by a federal entity obtained in connection with activities authorized in this title."

***Non-Federal Entity Cyber Threat Information Sharing with the Federal Government***

The Act designates DHS as the recipient of cyber threat information and, as such, the Secretary of Homeland Security must develop and implement the "capability and process" for receipt of the information. The Act authorizes the President, following a certification and explanation to Congress, to designate another federal entity, other than the Department of Defense (including the National Security Agency), to develop and implement an additional capability and process to receive cyber threat information.

Sharing cyber threat information with the federal government will not constitute a waiver of any legal protections, including laws governing trade secrets. Such information also will be exempt from certain disclosure laws, such as the Freedom of Information Act (FOIA). However, once shared with the federal government, cyber threat information may be used not only for cybersecurity purposes or identifying a cybersecurity threat or vulnerability, but also for (1) responding to, preventing, or mitigating a specific threat of death, serious bodily harm, or serious economic harm, including a terrorist act or use of a weapon of mass destruction; (2) responding to, investigating, prosecuting, preventing, or mitigating a serious threat to a minor; or (3) preventing, investigating, disrupting, or prosecuting an offense arising out of certain cyber-related criminal activities. This subsequent use of cyber threat information was one of the most contentious elements of the conference committee, and although this scoping may be broader than privacy advocates would have preferred, it is narrower than the Senate-passed version of the information sharing bill.

***Liability Protection***

Private entities that engage in monitoring activities or share or receive cyber threat information in conformance with the Act will be protected from liability for those actions.

***Sunset Period***

The Act will sunset on September 30, 2025.

---

[1] The Cybersecurity Act of 2015 also imposes requirements on federal government entities with regard to cybersecurity that do not apply to non-governmental entities and so are not addressed here.

## Contact Us

Mary Ellen Callahan, Partner, Jenner & Block

Phone: 202 639-6064 Email: mecallahan@jenner.com Download V-Card

Mary Ellen Callahan chairs Jenner & Block's Privacy and Information Governance Practice and provides privacy and data security counseling to a broad range of clients, including some of the most visited Internet websites. She served as Chief Privacy Officer of the US Department of Homeland Security from 2009 until August 2012 and received the 2013 Privacy Vanguard Award.


## Nancy C. Libin, Partner, Jenner & Block

Phone: 202 639-6086 Email: nlibin@jenner.com Download V-Card


Nancy C. Libin is a partner in the Privacy and Information Governance and Communications, Internet & Technology Practices. A former Chief Privacy and Civil Liberties Officer at the US Department of Justice, her practice encompasses law and policy with a focus on consumer protection and privacy, as well as national security and cybersecurity issues.


## Heidi L. Wachs, Special Counsel, Jenner & Block

Phone: 202 639-6081 Email: hwachs@jenner.com Download V-Card


Heidi L. Wachs is a special counsel in the firm's Privacy and Information Governance Practice. A nationally recognized leader in privacy, breach response, and data security compliance, her wealth of experience includes serving as a privacy researcher and as chief privacy officer of a major university.