LATHAM&WATKINS

Client Alert Commentary

Latham & Watkins Data Privacy, Security and Cybercrimes Practice

February 18, 2016 | Number 1927

# What You Need to Know About the Cybersecurity Act of 2015

***Legislation may change the way government and the private sector collaborate on cybersecurity.***

After years of vigorous debate and numerous false starts, in the closing hours of its 2015 session, the US Congress unceremoniously passed — and President Barack Obama signed — landmark cybersecurity information sharing legislation. The bill, the Cybersecurity Act of 2015 (the Act), first passed the House in April 2015 and later, in varied form, the Senate in October. A conference committee representing the intelligence and homeland security committees negotiated a consensus version of the legislation that was ultimately included as a rider on the omnibus Consolidated Appropriations Act, 2016.[1] While the Cybersecurity Act of 2015 is the result of many compromises and is based upon a voluntary sharing program, the result may nevertheless change the way government and the private sector collaborate on cybersecurity. The US Department of Homeland Security has commenced implementation of the information sharing provisions of the bill this month,[2] so the time is right for businesses to consider the potential implications for their cybersecurity readiness.

## Cybersecurity Information Sharing

The Cybersecurity Act of 2015 is divided into three primary subparts, the first of which creates a framework for information sharing between and among the public and private sectors. This framework, known as the Cybersecurity Information Sharing Act of 2015, or CISA, is an attempt to solve a universally recognized problem: corporate victims of cyberattacks — while often the best resources for actionable information to prevent future attacks — are hesitant to share information that may expose them to civil or criminal liability, embarrassment, loss of trust or competitive threats. CISA is an attempt to alleviate many of these impediments in hopes of fostering "greater cooperation and collaboration" to combat cyber threats.[3]

CISA authorizes private companies to share cybersecurity threat information for "cybersecurity purposes" with the federal government, and with other private entities. A "cybersecurity purpose" is defined as "the purpose of protecting an information system or information that is stored on, processed by, or transiting an information system from a cybersecurity threat or security vulnerability."[4] The Department of Homeland Security will be the federal government's clearinghouse for receiving and evaluating cyber threat information from private companies, and new procedures will be announced later this year to facilitate that process. CISA authorizes private companies to "monitor their information systems, operate defensive measures, and share and receive cyber threat information"[5] on a purely voluntary basis. Importantly, when companies share threat information with the federal government, they do not waive privilege; companies can declare information shared as proprietary and confidential, and know that the threat information shared will not be subject to state or local freedom of information requests. The CISA

specifies that private entities sharing cyber threat information with one another for cybersecurity purposes are not violating antitrust laws. Furthermore, Section 106 provides liability protection for private companies who monitor, share or receive threat information in accordance with CISA.[6] However, all information shared must be stripped of non-cybersecurity related information, and may be used by the federal government to prevent serious threats to minors, bodily harm, death, terrorism or serious economic harm, or to prosecute offenses arising under other cyber-related statutes.

CISA also clarifies that the private sector may not undertake offensive cybersecurity efforts such as "hacking back."[7] While most experts have never doubted the illegality of offensive cyber responses under current law, CISA makes clear that only defensive measures are authorized for cybersecurity purposes. Section 105 of the CISA also grants the President power to designate an agency other than the Department of Defense to develop additional information receiving procedures.[8] Early this year, Homeland Security and the Department of Justice will release procedures detailing when and how federal agencies may use the threat information they receive from the private sector, establishing guidelines intended to protect individual privacy and civil liberties.

Similarly, Homeland Security, the Department of Defense and the Office of the Director of National Intelligence will develop procedures for the timely sharing of cyber threat information from the federal government in real time. This framework will build on several years of pilot programs — part of a multi-agency effort under the umbrella of Homeland Security's Enhanced Cybersecurity Services program — that have already streamlined information sharing between the defense industrial base and commercial internet service providers.[9] This allows CISA to build on the existing role of Homeland Security's National Cybersecurity and Communications Integration Center (NCCIC), which itself was ratified by the National Cybersecurity Protection Act of 2014.[10] Homeland Security's Automated Indicator Sharing initiative builds on NCCIC's role as both the receiving point and distribution center for cyber threat information, and will allow the private sector to benefit in near real-time from the data federal agencies collect. Notably, this information sharing will be available not only to US entities, but to foreign governments and private sector entities as well.[11]

The Act preempts any state or local laws restricting or regulating CISA-related activities, with the exception of law enforcement practices and procedures. Agency heads, Inspectors General and the Comptroller General will submit oversight reports and implementation recommendations to Congress on how the federal government receives and shares cyber threat information. Additionally, the Director of National Intelligence and heads of intelligence agencies will report to Congress on the substance of cybersecurity threat information. CISA sunsets on September 30, 2025.

For the private sector, CISA creates a new opportunity to review when and how cyber threat information is shared. For many businesses, removing antitrust fears may be enough to promote sharing with their peers, but removing Freedom of Information Act discoverability, clarifying that legal privileges are not waived, and, critically, the limited immunity from regulatory action or civil liability, should spur many businesses to consider new ways of sharing threat intelligence with the government. While these sharing programs remain completely voluntary and subject to collective action problems, the reduction of risks — both real and perceived — may carry significant weight. And, as the government allows easier and faster actionable threat intelligence from itself and others, justifying not receiving this information either directly or through participation in an industry group (such as the sector-specific information sharing and analysis center) becomes more difficult.

## Changes to Federal Cybersecurity Practices

The Act also incorporates three separate pieces of legislation, each intended to address cybersecurity for the federal government. First, the National Cybersecurity Protection Advancement Act of 2015 enhances the role of the NCCIC, branding it the "federal civilian interface for multi-directional and cross-sector information sharing related to cybersecurity risks, incidents, analysis and warnings for federal and non-federal entities."[12] NCCIC will engage international partners, conduct preparedness exercises, and collaborate with state and local government to assess and evaluate threat information regarding public safety communications. NCCIC is also permitted to enter into information sharing relationships with non-federal entities. The NCCIC director will now report directly to the Secretary of Homeland Security in the event of "significant" cyber incidents.

Second, the Federal Cybersecurity Enhancement Act of 2015 is inward facing within the federal government. Since 2003, Homeland Security has been deploying traffic monitoring equipment and intrusion detection and prevention technology across the federal government networks. Interagency resistance and funding gaps have limited this technology — known as EINSTEIN — to covering only 45% of federal network access points.[13] The Act requires Homeland Security to "make [EINSTEIN] available" to all federal agencies within one year, and thereafter requires all agencies to "apply and continue to utilize the capabilities" across their networks. Whether the necessary appropriations will be distributed to meet this deadline is unclear. Agency heads are also subject to a two-month rolling time frame from the time new security features become available to their agency, to implement the changes on their networks. This part of the Act will sunset in seven years.

Third, the Federal Cybersecurity Workforce Assessment Act of 2015 requires the head of every federal agency to identify all positions within their agency that perform cybersecurity, or other cyber-related functions, and report to Congress how many workers in those roles have the proper security certifications, how many are ready to take certification exams, and how the agency plans to fill any certification and training gaps. Agency heads must also identify to the Director of the Office of Personnel Management (OPM) any information technology, cybersecurity or other cyber-roles of critical need in their agencies. Within two years, the Director of OPM will report to Congress on the agency heads' findings.

Finally, the Act also requires select federal agencies to produce written reports on cybersecurity. Homeland Security must study the threats to mobile devices the federal workforce and state emergency response providers use; Health and Human Services must report on how the healthcare industry prepares for cybersecurity threats; and the State Department must report on strategies for shaping US international cyberspace policy, and "consult" with countries that host known cyber criminals to determine what efforts have been made to "apprehend, prosecute, or otherwise prevent" future cybercrimes.[14]

While these changes to federal practice may have little direct impact on the private sector, increased attention and spending on federal cybersecurity will improve the health of the overall ecosystem, and potentially advance defensive measures available to the private sector. In addition, each time Homeland Security deploys more intrusion detection and prevention technology, the government's visibility into the cyber threat increases, along with the value of the government's threat reporting. All of these efforts will be furthered by the President's recently announced Cybersecurity National Action Plan, or CNAP, which carries out last year's Cybersecurity Strategy and Implementation Plan. In large part CNAP focuses on the basics; upgrading federal information technology, expanding existing programs and enhancing the public's cybersecurity awareness.[15] But the plan, backed by a US$19 billion budget request, also creates a government-wide Chief Information Security Officer to oversee these efforts, as well as a non-governmental commission that will be tasked with making cybersecurity recommendations for the next decade. Securing an enterprise network, whether it belongs to the US government or a large corporation,

is an evolving effort that takes investments of time and capital, buoyed by the collective action of individuals and business partners. If the Cybersecurity Act of 2015 helps to further broaden cybersecurity collaboration, the security of all participating networks may well take a significant step forward.

On February 16, the Department of Homeland Security transmitted four reports to Congress on cybersecurity information sharing and interim privacy protections. These guidance documents set in motion the ability for the private sector to share cybersecurity information with the government and describe how the government will use and share threat indicators, while also managing privacy concerns.[16]

---

If you have questions about this *Client Alert*, please contact one of the authors listed below or the Latham lawyer with whom you normally consult:


**Manuel A. Abascal**
manny.abascal@lw.com
+1.213.891.7889
Los Angeles, CA

**Jennifer C. Archie**
jennifer.archie@lw.com
+1.202.637.2205
Washington, D.C.

**Gail E. Crawford**
gail.crawford@lw.com
+44.20.7710.3001
London, UK

**Benjamin A. Naftalis**
benjamin.naftalis@lw.com
+1.212.906.1713
New York, New York

**David J. Schindler**
david.schindler@lw.com
+1.213.891.8415
Los Angeles, CA

**Scott C. Jones**
scott.jones@lw.com
+1.202.637.3316
Washington, D.C.

**Alexander L. Stout**
alexander.stout@lw.com
+1.202.637.2158
Washington, D.C.


**You Might Also Be Interested In**

Privacy Blog: Proposal of EU-US Privacy Shield Leaves Businesses in State of Uncertainty

7 Tips for Conducting Effective Cybersecurity Due Diligence in M&A Transactions

Cybersecurity regulation and best practice in the US and UK

The USA Freedom Act: What it Changes and (Mostly) Doesn't for Cloud Services – And is it Really the Issue

---

**Endnotes**

---

[1] Consolidated Appropriations Act, 2016, Pub. L. No. 114-113, Div. N, Title I (2015).

[2] *See* http://blogs.wsj.com/cio/2016/02/03/wsj-cio-network-dhs-to-start-sharing-cybersecurity-threat-indicators-with-industry/

[3] 161 Cong. Rec. S8848 (daily ed. Dec. 18, 2015)(statement of Sen. Burr).

[4] Cybersecurity Act of 2015, § 102.

[5] *Id.*

[6] *Id.*

[7] *Id.*

[8] *Id.*

[9] *See* https://www.dhs.gov/sites/default/files/publications/privacy-pia-28-a-nppd-ecs-november2015.pdf.

[10] National Cybersecurity Protection Act of 2014, Pub. L. No. 113-282, 128 Stat. 3066 (2014).

[11] *See* https://www.dhs.gov/sites/default/files/publications/privacy-pia-nppd-ais-october2015.pdf.

[12] 161 Cong. Rec. S8849.

[13] *See* http://www.federaltimes.com/story/government/cybersecurity/2015/08/10/opm-breach-kick-starts-einstein-efforts/31424351/.

[14] 161 Cong. Rec. S8850.

[15] *See* https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan.

[16] *See* https://www.us-cert.gov/sites/default/files/ais_files/Privacy_and_Civil_Liberties_Guidelines_%28Sec 105%28b%29%29.pdf; https://www.us-cert.gov/sites/default/files/ais_files/Operational_Procedures_%28105%28a%29%29.pdf; https://www.us-cert.gov/sites/default/files/ais_files/Non-Federal_Entity_Sharing_Guidance_%28Sec%20105%28a%29%29.pdf ;https://www.us-cert.gov/sites/default/files/ais_files/Federal_Government_Sharing_Guidance_%28103%29.pdf.