A New Cybersecurity Regime and a New Regulation to Mandate Secure Information Systems for Government Contractors

By C. Joël Van Over and Travis L. Mullaney

Congress has enacted a recent wave of legislation to address ongoing cybersecurity threats; the Executive Branch, on May 12, 2016, adopted new cybersecurity regulations; and other Federal initiatives are underway and will bring additional promised change requiring enhanced cybersecurity protections.

The Cybersecurity Act of 2015 ("Cybersecurity Act") presents the federal government's first successful step toward creating a partnership between government and private industry to address cybersecurity issues.[1] Although Congress struggled for years to pass legislation to address the geometric increase in cybersecurity threats, this is the first major cybersecurity legislation to succeed in bringing private industry and domestic nonfederal entities into a federal initiative directed at sharing information on cyber threat "indicators" detected and defensive measures taken to protect information systems and information accessible through or controlled by information systems. The key language of Title I of the Cybersecurity Act was taken from an earlier controversial bill known as the Cybersecurity Information Sharing Act (CISA),[2] which was included with three other Titles that comprise the Cybersecurity Act. The consolidated Act was enacted as part of the FY2016 omnibus appropriations bill to ease passage through Congress. The Cybersecurity Act was signed into law on December 18, 2015.

Notwithstanding the delay in passing comprehensive cybersecurity legislation, the Executive Branch was well prepared for its passage, due in part to the federal actions mandated by the Federal Information Security Modernization Act of 2014 (FISMA).[3] Many of the new Executive Branch initiatives implement the Cybersecurity Act, and others are farther reaching, continuing executive branch work described in the Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government.[4] For example, while the Cybersecurity Act contemplates only voluntary reporting of cyber threat indicators and defensive measures, recent Department of Defense (DoD) regulations require covered federal contractors to report cyber incidents. These recent DoD regulations, implemented as part of the Defense Federal Acquisition Regulation Supplement (DFARS) require strengthening information systems through compliance with NIST SP 800-171 information system cybersecurity standards related to contract performance and adopt a new DoD policy on the acquisition of cloud computing services, all with

associated contract clauses.[5] Finally, on May 16, 2016, a final rule was published amending the Federal Acquisition Regulations (FAR) "to add a new subpart and contract clause for the basic safeguarding of contractor information systems that process, store or transmit Federal contract information." This new, far-reaching, mandatory regulation is also discussed below. Mandatory reporting of cyber incidents for covered Executive agency contracts, similar to the recent DFARS requirements, may be expected.

Understanding the contours of the Cybersecurity Act, the new FAR regulation on safeguarding contractor information systems, and recent initiatives since passage of the Cybersecurity Act, are important to preparing for change.

Recent Cybersecurity Initiatives and New Regulations

The President and designated agencies took swift action to invigorate and implement the Cybersecurity Act. On February 9, 2016, the President announced the implementation of a Cybersecurity National Action Plan (CNAP), the culmination of a seven-year effort to strengthen cybersecurity, and issued an Executive Order creating the Commission on Enhancing National Cybersecurity (the "Commission") as a central feature of CNAP, within the Department of Commerce.[6] On April 13, 2016, the President announced the members of the Commission, selected by the President and bipartisan Congressional leadership.[7] The National Institute of Standards and Technology (NIST) and its National Cybersecurity Center of Excellence (NCCoE), also seated within the Department of Commerce, will provide significant resources to the Commission.[8] NIST is currently publishing Federal Register Notices concerning monthly open meetings held by the Commission. The first meetings were held on April 14, 2016 in Washington DC, and May 6, 2016 in New York City, at the New York University Center for Law. Watch for upcoming NIST Notices of future open meetings held by the Commission.

NIST also awarded a $29M indefinite delivery/indefinite quantity contract to MITRE Corp. to support the NCCoE, and MITRE has published a Common Attack Pattern Enumeration and Classification resource, which will be helpful in establishing a common cyber threat vocabulary, as various agencies continue to implement guidance.[9] The NCCoE provides another NIST resource, as one of NCCoE's missions is to collaborate with industry to identify the nation's most pressing cybersecurity issues, generate a detailed technical description of each issue, and work with technology vendors to develop a standards-based example solution to address those issues. This work will offer private companies both informal access to the planning process and also contracting opportunities to participate directly in this process.[10]

On February 16, 2016, the Department of Homeland Security and the Department of Justice issued preliminary substantive guidance concerning the implementation of the Cybersecurity Act, comprised of four draft documents discussing cyber threat indicators and defensive measures, as well as privacy issues.[11] This guidance is summarized below.

The new May 16, 2016 final FAR regulation, 48 C.F.R. Part 4.19, and the associated contract clause, establish minimum safeguarding requirements for federal contractor information systems and expressly provide that additional specific requirements may be imposed by Federal agencies and departments. The new FAR regulation goes into effect on June 16, 2016.

In the category of regulatory action that is still incomplete is the proposed rule published by the Information Security Oversight Office of the National Archives and Records Administration (NARA) on May 8, 2015 to implement the Executive Branch Controlled Unclassified Information (CUI) Program and Executive Order 13556 (2010) within the Federal Government. This proposed rule would establish a government-wide policy on "designating, safeguarding, disseminating, marking, decontrolling, and disposing of" CUI.[12] While

no final rule has issued, NIST issued SP 800-171 in June 2015, entitled *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations*, and as noted above, DoD amended its regulations to require covered contractors to comply with this recent NIST standard through its final interim regulations and contract clauses, DFARS 252.204-7008-9 and 7012, on December 30, 2015.[13] The extent to which the anticipated final NARA regulation will adopt NIST SP 800-171 is not clear. New cybersecurity requirements related to classified information have also been anticipated for well over a year, since DoD announced (but has not yet adopted), Conforming Change 2 to the National Industrial Security Program Operating Manual (NISPOM).

Key Elements of the Title I Information Sharing Provisions of the Cybersecurity Act of 2015

The primary goal of the Cybersecurity Act is to facilitate the voluntary exchange of information regarding cybersecurity threats between and among the federal government and the private sector. The Cybersecurity Act directs federal agencies[14] to establish procedures for the sharing of cybersecurity and threat information and protects private entities from liability should they elect to share cybersecurity information with the government.

Covered Cybersecurity Information

The types of information to be shared under the Act include:

- "Cybersecurity Threat": "an action, not protected by the First Amendment to the Constitution of the United States, on or through an information system that may result in an unauthorized effort to adversely impact the security, availability, confidentiality, or integrity of an information system or information that is stored on, processed by, or transiting an information system[15]."
- "Cybersecurity Threat Indicator": includes information describing or identifying any type or attribute of a cybersecurity threat, including malicious reconnaissance, methods of defeating a security control or exploiting a vulnerability, methods of causing an authorized user to unwittingly defeat a security control or exploit a vulnerability, malicious cyber command and control, and actual harm or potential harm caused by an incident, including exfiltrated information.
- "Defense Measure": "an action, device, procedure, signature, technique, or other measure applied to an information system or information that is stored on, processed by, or transiting an information system that detects, prevents, or mitigates a known or suspected cybersecurity threat or security vulnerability."[16]

The Department of Homeland Security (DHS) has been tasked with developing the appropriate policies and procedures related to the receipt of cyber threat indicators and defense measures by the Federal Government as well as guidelines for entities sharing cyber threat indicators with the Federal Government. The goal is to establish real time notification of cybersecurity threat indicators and sharing of cybersecurity threat information, and this effort has been rapidly implemented.[17] DHS has implemented the Security Cyber Threat Indicator and Defensive Measures Submission System, which offers a form for submitting information electronically.[18]

Given the amount of information DHS expects to receive and to share under the Act, it will also be critical that both the government and private entities maintain appropriate security controls for the handling and retention of such information to prevent unauthorized disclosure of or access to such information. Among other things, both governmental and private entities are instructed to review cyber threat indicators and related information to assess whether such information contains personally identifiable information and to

remove such information not directly related to a cybersecurity threat prior to sharing. Federal entities must also remove any personal information of a specific individual or information that identifies a specific individual and all other information not directly related to a cybersecurity threat before sharing information with relevant federal and non-federal entities.[19]

Use of Information

Designated federal agencies are required to develop procedures for timely sharing information in the Federal Government's possession concerning cyber threat indicators, defensive measures and information related to cybersecurity threats that are classified with representatives of federal and nonfederal entities with appropriate security clearances, and those that are unclassified, including controlled unclassified information to federal and nonfederal entities, and to the public, if appropriate. Such procedures should also facilitate and promote the periodic sharing "through publication and targeted outreach, of cybersecurity best practices that are developed based on ongoing analyses of cyber threat indicators, defensive measures, and information relating to cybersecurity threats" in the possession of the Federal Government.[20]

A private entity's use of information received under the Act is limited to use for "cybersecurity purposes," meaning "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." A private entity is expressly authorized to monitor systems and operate defense measures for cybersecurity purposes on its own systems or other systems with the written consent of the owner, including the Federal Government, subject to restrictions that apply to classified information.[21] The term "monitor" is defined to mean "to acquire, identify, or scan, or to possess, information that is stored on, processed by, or transiting on and information system.[22] Nonfederal entities are expressly authorized to share and receive with each other (and with the Federal Government) cyber threat indicators and defensive measures for cybersecurity purposes as long as they comply with lawful restrictions placed on the sharing of such information by the sharing entity.[23]

Federal, state, and local authorities are prohibited from using information shared under the Act to take any regulatory or enforcement action towards a private entity. Although the exchange of information between private entities related to cyber threat indicators, defense measures, and the like is nominally exempted from anti-trust enforcement under the terms of the Act,[24] any exchanges of price or cost information, customer lists, or information regarding future competitive planning that leads to price-fixing or an attempt to monopolize a market may nevertheless receive regulatory scrutiny.[25]

Protection from Liability

Section 106, entitled "Protection from Liability" lays out the relevant protections provided to private entities for conducting activities in accordance with the Act. Subsection (a) protects against liability for monitoring of systems and information and subsection (b) protects against liability for the sharing or receipt of a cyber threat indicator or defense measure, in each case if the monitoring, sharing, and/or receipt was conducted in accordance with the provisions of the Act.[26]

No Duty to Share

Sharing and receipt of cybersecurity threat information is a tool at a private entity's disposal under the Cybersecurity Act, but sharing is voluntary and participation is not required.[27] Federal agencies cannot condition the award of a contract on sharing of cyber threat indicators,[28] and there is no liability for non-

participation.[29] However, the Cybersecurity Act does not prohibit agencies from independently adopting regulations that require the reporting of cybersecurity incident information by federal contractors, as DoD has done, and as other agencies and Departments may do in the future.

Interim Guidance on Implementation

On February 16, 2016, DHS, in conjunction with the Department of Justice (DOJ), the Department of National Intelligence (DNI) and the Department of Defense (DoD), issued substantive interim guidance documents governing implementation of the Cybersecurity Act.[30] Final guidance must be issued 180 days after the enactment of the Cybersecurity Act; thus, it is possible that the interim guidance may be amended or augmented in June 2016. The interim guidance documents provide federal agencies and the private sector with a clearer understanding of how to identify and share cyber threat indicators and defensive measures with DHS's National Cybersecurity and Communications Integration Center (NCCIC) and how the NCCIC will share and use that information. The published documents include four separate sets of guidance, guidelines and procedures:

- Guidance to Assist Non-Federal Entities to Share Cyber Threat Indicators and Defensive Measures with Federal Entities[31]
    - Identifies the type of information that would qualify as a cyber threat indicator under the Cybersecurity Act, as well as information that is not directly related to such information such as personal information of a specific individual or information that identifies a specific individual;
    - Identifies the types of information protected under otherwise applicable privacy laws that are unlikely to be directly related to a cybersecurity threat;
    - Explains how to identify and share defensive measures;
    - Explains the DHS Automated Indicator Sharing (AIS) program, as well as web form and email intake capabilities.
- Privacy and Civil Liberties Interim Guidelines[32]
    - Explain the obligations of federal entities to assess, protect and remove known personal information before disseminating cyber threat or defensive measures or other information authorized for sharing under the Cybersecurity Act;
    - Review Fair Information Practice Principles (FIPPS) as defining principles to be used in evaluating systems that affect individual privacy;
    - Require federal entities to timely review information received as a cyber threat indicator and destroy personal information and information known not to be directly related to uses authorized by the Cybersecurity Act;
    - Require federal entities to notify those who have received a cyber threat indicator or defensive measure from a federal entity if the information was provided in error;
    - Require federal entities to notify a U.S. person whose personal information is known to have been shared in violation of the Cybersecurity Act.

  - Require federal entities to share cyber threat indicators and defensive measures using specific secure information sharing architecture and access control markings.

- Interim Procedures Related to the Receipt of Cyber Threat Indicators and Defensive Measures by the Federal Government[33]

  - Prescribe the processes and specifications for receiving, handling, and sharing information pursuant to the Cybersecurity Act;

  - Specify procedures for standardizing and changing AIS profile submissions of cyber threat indicators and defensive measures.

- Interim Guidance on Sharing of Cyber Threat Indicators and Defensive Measures by the Federal Government[34]

  - Describes federal programs for sharing classified cyber threat indicators and defensive measures;

  - Describes policies for timely sharing of declassified and unclassified cyber threat indicators and defensive measures, and the programs used to share such information by federal entities.

These guidance documents set forth additional details regarding implementation of the Cybersecurity Act and further guidance is expected in the future.

Final Federal Acquisition Regulation: Basic Safeguarding of Covered Contractor Information Systems

The new FAR 4.19, and implementing contract clause 52.204-21, apply to all federal contractor information systems that "are owned or operated by a contractor that processes, stores, or transmits Federal contract information." The new regulation applies to all acquisitions, including commercial item acquisitions, other than for commercial off the shelf (COTS) items. The new regulation applies to subcontractors at any tier whose information systems are covered by the definitions, subject to the COTS exception. The Federal Register final rule explains that the new rule is intended to ensure "a basic level of safeguarding for any contractor system with Federal information, reflective of actions a prudent business person would employ" and "is just one step in a series of coordinate regulatory actions being taken or planned to strengthen protections of information systems." It is clear that more regulations will follow.

While the new regulation does not require compliance with any specific NIST standards, unlike the recent DoD regulation that requires NIST SP 800-171 compliance, the new regulation lists many of the same 14 families of security requirements listed in NIST SP 800-171, and all of the new regulation requirements have analogs in NIST SP 800-171. If a contractor complies with NIST 800-171, it will comply with the new regulation.

The Definitions that Define the Scope of FAR 4.19

The new rule is focused on systems and not particular information or data and covers even those systems "incidental to providing a product or service for an agency…" In other words, the new regulation is very broad, as the definitions suggest.

"Covered contractor information system means an information system that is owned or operated by a contractor that processes, stores, or transmits Federal contract information."

"Federal contract information means information, in intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government, but not including information provided by the Government to the public (such as that on public websites) or simple transactional information, such as that necessary to process payments."

"Information means any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual (Committee on National Security Systems Instruction (CNSSI) 4009)."

"Information system means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information (44 U.S.C. 3502)."

"Safeguarding means measures or controls that are prescribed to protect information systems."

Mandatory Minimum Basic Safeguarding Security Controls

The new regulation lists 15 mandatory security controls, which must be implemented, "at a minimum." Nine of the security requirements relate to access control and authentication of authorized users, some very specific and some more general in nature. Access controls must be robust. For example, user access must be controlled and tracked, and access must be compartmentalized physically and logically, to limit access to those portions of the system, and to transactions and functions, that a user is authorized to access. Publically accessible system components must be separated from internal networks. Organizational communications must be monitored, controlled and protected "at the external boundaries and key internal boundaries of the information system." In addition, "information system flaws" must be "identified, reported and corrected" in a timely manner. Protections from malicious code must be implemented and updated at "appropriate locations within organizational information systems." Finally, "periodic scans of the information system and real time scans of files from external sources" must be performed.

The background section of the final FAR 4.19 rule provides that "we plan to develop regulatory changes for the FAR in coordination with National Archives and Records Administration (NARA) which is separately finalizing a rule to implement Executive Order 13556 addressing CUI." The NARA proposed rule to adopt the proposed 32 C.F.R. 2002, published on May 8, 2015, remains pending. The proposed FAR rule on CUI has not yet been published in the Federal Register.

Effect on Government Contractors

Based upon the Cybersecurity Act of 2015, the new FAR regulation implementing Basic Safeguarding of Covered Contractor Information Systems, and the other Federal initiatives described in this Advisory, 2016 promises to be an active year in the Federal cybersecurity arena. While the reporting of cyber threat indicators and defensive measures contemplated by the Cybersecurity Act are voluntary, the recent DFARS 252.204-7008 and 7012 makes such reporting mandatory and requires covered contractors to comply with NIST SP 800-171. It is possible, if not likely, that such reporting will become mandatory for non-DoD contractors when NARA and the FAR Council coordinate the implementation of protections for CUI on contractor systems. We recommend that all potentially affected federal contractors attend one of the upcoming public meetings to be held by the newly established Commission on Enhancing National Cybersecurity to learn more about plans and how potential new NIST standards may affect federal

contractors. Watch for our upcoming Alerts and Advisories as federal initiatives evolve, and call us with questions.

If you have any questions about the content of this Advisory, please contact the Pillsbury attorney with whom you regularly work, or the authors below.

C. Joël Van Over (bio)
Northern Virginia
+1.703.770.7604
joel.vanover@pillsburylaw.com

Travis L. Mullaney (bio)
Northern Virginia
+1.703.770.7751
travis.mullaney@pillsburylaw.com

1 The four titles that comprise the Cybersecurity Act consolidate proposed legislation originating in both the Senate and the House of Representatives. Title I retains the name of a bill passed by the Senate in October 2015: the Cybersecurity Information Sharing Act of 2015; Title II has two subtitles that retain then names of bills, passed by the House in April 2015 and favorably reported from the Senate Committee on Homeland Security and Governmental Affairs in July 2015: the National Cybersecurity Protection Advancement Act of 2015 and the Federal Cybersecurity Enhancement Act of 2015,respectively; Title III retains the name of a bill introduced by the Senate in August 2015 and referred to Senate Committee on Homeland Security and Governmental Affairs. Title IV directs various agencies to take specific actions related to mobile device security, international cybersecurity policy strategy, emergency response provider interoperability related to cybersecurity, preparedness of the health care industry to respond to cybersecurity threats, and the security of federal national security systems and systems that provide access to personally identifiable information. The final provision of the Title IV enables the Federal Government to prosecute overseas criminals who profit from financial information stolen from Americans. *See* U.S. Congress, Joint Explanatory Statement to Accompany the Cybersecurity Act of 2015 (Dec. 18, 2015), *available at* https://www.congress.gov/congressional-record/2015/12/18/senate-section/article/s8844-1.

2 *See* Cybersecurity Information Sharing Act, 6 U.S.C. § 1501, et seq.

3 44 U.S.C. § 3531, et seq.

4 The CSIP resulted from long awaited OMB Guidance. The CSIP, issued as a Presidential Memorandum on October 30, 2015, in conjunction with a second Presidential Memorandum, Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements, in response to FISMA mandates. *See* OMB, Memorandum M-16-04, Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government (Oct. 30, 2015), *available at* https://www.whitehouse.gov/sites/default/files/omb/memoranda/2016/m-16-04.pdf (last accessed May 19, 2016); *see also* OMB, Memorandum M-16-03, Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements (Oct. 30, 2015), *available at* https://www.whitehouse.gov/sites/default/files/omb/memoranda/2016/m-16-03.pdf.

5 *See* DFARS 252.204-7008, 7009, and 7012; and DFARS 239.76, 252.239-7009-7010. *See also* C. Joël Van Over et al., Client Advisory: Government Contractor Brace for Continuing Changes in Cybersecurity Regulations (Feb. 2, 2016), *available at* http://www.pillsburylaw.com/publications/government-contractors-brace-for-continuing-changes-in-cybersecurity-regulations.

6 *See* White House Office of Press Secretary, FACT SHEET: Cybersecurity National Action Plan (Feb. 9, 2016), *available at* https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan (last accessed May 19, 2016); *see also* Executive Order, Commission on Enhancing National Cybersecurity (Feb. 9, 2016), *available at* https://www.whitehouse.gov/the-press-office/2016/02/09/executive-order-commission-enhancing-national-cybersecurity.

7 *See* Michael Daniel, Special Assistant to the President and Cybersecurity Coordinator, et al., Announcing the President's Commission on Enhancing National Cybersecurity, White House Blog (Apr. 13, 2016), *available at* https://www.whitehouse.gov/blog/2016/04/13/announcing-presidents-commission-enhancing-national-cybersecurity.

8 The NCCoE partners with companies, academics, and federal agencies, and published helpful guides addressing various threat scenarios and solutions helpful to various business sectors, including health, retail, IT vendors and users. *See* generally https://nccoe.nist.gov (last accessed May 19, 2016).

9 NIST also awarded a $29M IDIQ to MITRE to support the NCCoE, and MITRE has published a Common Attack Pattern Enumeration and Classification resource, *available at* https://capec.mitre.org/data/definitions/3000.html.

10 *See* generally https://nccoe.nist.gov.

11 *See* infra notes 30 to 34.

12 ISOO, Proposed Rule, Controlled Unclassified Information, 80 Fed. Reg. 26501 (May 8, 2015), *available at* https://federalregister.gov/a/2015-10260 (last accessed May 19, 2016).

13 *See* Client Advisory: Government Contractor Brace for Continuing Changes in Cybersecurity Regulations, supra n.5.

14 A Department of Homeland Security Cyber Threat Indicator and Defensive Measures Submission System offers a form for submitting information. *See* http://www.us-cert.gov/forms/share-indicators (last accessed May 19, 2016). The Cybersecurity Act defines "Appropriate Federal Entities" as the Departments of Commerce, Defense, Energy, Homeland Security, Justice, Treasury, and the Office of the Director of National Intelligence. *See* Cybersecurity Information Sharing Act, supra n.2, at 6 U.S.C. § 1501(3).

15 The term "information system" as defined in the Cybersecurity Act adopts the broad definition in 44 U.S.C. 3502, and "means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information." *See id.* at §1501(9). The definition expressly includes industrial control systems other control systems. *Id*.

16 *See id*. at § 1501(7).

17 *Id.* at § 1502(b);

18 *See* http://www.us-cert.gov/forms/share-indicators.

19 *See* 6.U.S.C. § 1502(b)(1)(E).

20 *Id.* at § 1502(a).

21 *Id.* at § 1503 (a) and (b).

22 *Id.* at § 1501 (Definitions).

23 *Id.* at § 1503(c).

24 *Id.* at § 1503(e).

25 *Id.* at § 1507(e).

26 *Id.* at § 1505(a)-(b).

27 *See id.* at § 1507(h)(1).

28 *See id*. at § 1507(h)(3).

29 *See id.* at § 1507(i).

30 *See* DHS, National Protection and Programs Directorate; Cybersecurity Information Sharing Act of 2015 Interim Guidance Documents-Notice of Availability, 81 Fed. Reg. 8214 (Feb. 16, 2016), *available at* https://federalregister.gov/a/2016-03430.

31 *See* DHS & DOJ, Guidance to Assist Non-Federal Entities to Share Cyber Threat Indicators and Defensive Measures with Federal Entities (Feb. 16, 2016), *available at* https://www.us-cert.gov/sites/default/files/ais_files/Non-Federal_Entity_Sharing_Guidance_%28Sec%20105%28a%29%29.pdf (last accessed May 19, 2016).

32 *See* DHS & DOJ, Privacy and Civil Liberties Interim Guidelines: Cybersecurity Information Sharing Act of 2015 (Feb. 16, 2016), *available at* https://www.us-cert.gov/sites/default/files/ais_files/Privacy_and_Civil_Liberties_Guidelines_%28Sec%20105%28b%29%29.pdf.

33 *See* DNI, DHS, DoD & DOJ, Sharing of Cyber Threat Indicators and Defensive Measures by the Federal

Government under the Cybersecurity Information Sharing Act of 2015 (Feb. 16, 2016), *available at* https://www.us-cert.gov/sites/default/files/ais_files/Federal_Government_Sharing_Guidance_%28103%29.pdf.

34 *See* DHS & DOJ, Interim Procedures Related to the Receipt of Cyber Threat Indicators and Defensive

Measures by the Federal Government (Feb. 16, 2016), *available at* https://www.us-cert.gov/sites/default/files/ais_files/Operational_Procedures_%28105%28a%29%29.pdf.

Pillsbury Winthrop Shaw Pittman LLP is a leading international law firm with offices around the world and a particular focus on the energy & natural resources, financial services, real estate & construction, and technology sectors. Recognized by *Financial Times* as one of the most innovative law firms, Pillsbury and its lawyers are highly regarded for their forward-thinking approach, their enthusiasm for collaborating across disciplines and their unsurpassed commercial awareness.