Congressional Research Service
Informing the legislative debate since 1914

Cybersecurity and Information Sharing: Comparison of H.R. 1560 (PCNA and NCPAA) and S. 754 (CISA)

Updated November 6, 2015

Congressional Research Service
https://crsreports.congress.gov
R44069

CRS REPORT
Prepared for Members and
Committees of Congress

Summary

Effective sharing of information in cybersecurity is generally considered an important tool for protecting information systems from unauthorized access. Five bills on such sharing have been introduced in the 114th Congress—H.R. 234, H.R. 1560, H.R. 1731, S. 456, and S. 754, and relevant provisions have appeared in other bills. The White House has also submitted a legislative proposal and issued an executive order on the topic.

H.R. 1560, the Protecting Cyber Networks Act (PCNA), and H.R. 1731, the National Cybersecurity Protection Advancement Act of 2015 (NCPAA), passed the House the week of April 20. The bills were then combined as separate titles in H.R. 1560.

In the Senate, S. 754, the Cybersecurity Information Sharing Act of 2015 (CISA), was reported in March and was proposed to be considered as an amendment to H.R. 1735, the National Defense Authorization Act (NDAA). More than 70 amendments to CISA were submitted, a managers amendment was circulated, and a cloture motion was filed on August 3. On August 5, a unanimous consent agreement was reached permitting consideration, and the Senate began debate on a manager's amendment on October 20. The substitute included several of the filed amendments. Several additional amendments were considered, but most did not succeed. The Senate passed CISA, as amended, on October 27. Presumably, any inconsistencies between CISA and the two titles of H.R. 1560 could be reconciled during the process for resolving differences between the House and Senate bills.

PCNA, NCPAA, and CISA have many similarities but also significant differences. All focus on information sharing among private entities and between them and the federal government. NCPAA would explicitly amend portions of the Homeland Security Act of 2002, and PCNA would amend parts of the National Security Act of 1947. CISA addresses the roles of the Department of Homeland Security and the intelligence community but does not explicitly amend either act. NCPAA and CISA also contain provisions relating to cybersecurity of federal agencies and their information systems and of critical infrastructure sectors. CISA also has provisions on international cybersecurity policy and cybercrime. The bills differ in how they define some terms in common, the roles they provide for federal agencies, processes for nonfederal entities to share information with the federal government, processes for protecting privacy and civil liberties, uses permitted for shared information, and reporting requirements.

All the bills would address concerns about barriers to sharing information about cybersecurity within and across sectors. Such barriers are considered by many to hinder protection of information systems. Private-sector entities often express reluctance to share such information because of concerns about legal liability, antitrust violations, regulatory requirements, and protection of intellectual property and other proprietary business information. Institutional and cultural factors have also been cited—traditional approaches to security tend to emphasize secrecy and confidentiality, which would necessarily impede sharing of information.

All the bills have provisions aimed at facilitating information sharing among private-sector entities and providing protections from liability. While reduction or removal of such barriers may provide benefits, concerns have been raised about potential adverse impacts, especially on privacy and civil liberties, and potential misuse of shared information. The bills address many of those concerns. In general, they limit the use of shared information to purposes of cybersecurity and law enforcement, and they limit government use, especially for regulatory purposes. All include provisions to shield information shared with the federal government from public disclosure and to protect privacy and civil liberties with respect to shared information that is not needed for cybersecurity purposes. All require reports to Congress on impacts of their provisions.

Most observers appear to believe that legislation on information sharing is either necessary or at least potentially beneficial—provided that appropriate protections are included—but additional factors may be worthy of consideration as the legislative proposals are debated. In particular, resistance to information sharing among private-sector entities might not be substantially reduced by the actions contemplated in the legislation; and information sharing is only one of many facets of cybersecurity that organizations need to address to secure their information systems.

Contents

Background 1
Current Legislative Proposals 3
House Consideration of NCPAA and PCNA 3
Senate Consideration of CISA 3
Other Legislative Proposals in the 114th Congress 4
Overview of the Legislative Proposals 4
Selected Issues 6
Side-by-Side Comparison of NCPAA, PCNA, and CISA 11
Glossary of Abbreviations in the Tables 12
Notes on the Tables 13

Tables

Table 1. Side-by-Side Comparison of Corresponding Sections in PCNA (Title 1) and NCPAA (Title II) of H.R. 1560 as Passed by the House and CISA, S. 754, as Passed by the Senate 15
Table 2. Summaries of Sections in NCPAA and CISA: Federal Cybersecurity 60
Table 3. Summaries of Sections in NCPAA and CISA: Critical Infrastructure Cybersecurity 67
Table 4. Summaries of Sections in NCPAA and CISA: Other Cybersecurity Provisions 71

Contacts

Author Information 72
Acknowledgments 72

This report compares two House bills and one Senate bill that address information sharing and related activities in cybersecurity. It also discusses some of the issues that those and other legislative proposals address. The three bills compared are

- the Protecting Cyber Networks Act (PCNA, H.R. 1560 as passed by the House),
- the National Cybersecurity Protection Advancement Act of 2015 (NCPAA, H.R. 1731 as passed by the House), and
- the Cybersecurity Information Sharing Act of 2015 (CISA, S. 754, as passed in the Senate).

All three bills focus on information sharing among private entities and between them and the federal government. They address the structure of the information-sharing process, issues associated with privacy and civil liberties, and liability risks for private-sector sharing, and they also address some other topics in common. In addition to other provisions, NCPAA would explicitly amend portions of the Homeland Security Act of 2002 (6 U.S.C. §101 et seq.), and PCNA would amend parts of the National Security Act of 1947 (50 U.S.C. §3021 et seq.). CISA has many similarities to a bill with a similar name introduced in the 113th Congress and shares many provisions with PCNA, although there are also significant differences between them.

This report consists of an overview of the three bills, other legislative proposals, and an executive order on information sharing, along with selected associated issues, followed by a side-by-side analysis of NCPAA, PCNA, and CISA.[1] For information on economic aspects of information sharing, see CRS Report R43821, *Legislation to Facilitate Cybersecurity Information Sharing: Economic Analysis*, by N. Eric Weiss. For discussion of legal issues, see CRS Report R43941, *Cybersecurity and Information Sharing: Legal Challenges and Solutions*, by Andrew Nolan. For an overview of cybersecurity issues, see CRS Report R43831, *Cybersecurity Issues and Challenges: In Brief*, by Eric A. Fischer

Note: Revisions in this update focus on changes to CISA resulting from Senate floor consideration of the bill. Future updates will include further analysis.

Background

Barriers to the sharing of information on threats, attacks, vulnerabilities, and other aspects of cybersecurity—both within and across sectors—have long been considered by many to be a significant hindrance to effective cybersecurity, especially with respect to critical infrastructure, such as the financial system and the electric grid.[2] Private-sector entities often claim that they are reluctant to share such information among themselves because of concerns about legal liability, antitrust violations, and potential misuse, especially of intellectual property, including trade secrets and other proprietary business information.

Perceived barriers to sharing with government agencies include concerns about risks of disclosure and the ways governments might use the information provided. In addition, some private-sector

[1] The analysis is limited to a textual and policy comparison of the bills and is not intended to reach any legal conclusions regarding them.

[2] See, for example, CSIS Commission on Cybersecurity for the 44th Presidency, *Cybersecurity Two Years Later*, January 2011, http://csis.org/files/publication/110128_Lewis_CybersecurityTwoYearsLater_Web.pdf. There are currently 16 recognized critical-infrastructure sectors (see The White House, "Critical Infrastructure Security and Resilience," Presidential Policy Directive 21, February 12, 2013, http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil).

entities complain that the federal government does not share its information—especially classified information—effectively with the private sector, and that there is little reciprocity or other incentives for such entities to share information with the government.[3]

Institutional and cultural factors have also been cited—traditional approaches to security tend to emphasize secrecy and confidentiality, which would necessarily impede sharing of information. While reduction or removal of such barriers may provide cybersecurity benefits, concerns have also been raised about potential adverse impacts, especially with respect to privacy and civil liberties.

A few sectors are subject to federal notification requirements,[4] but most such information sharing is voluntary, often through sector-specific Information Sharing and Analysis Centers (ISACs)[5] or programs under the auspices of the Department of Homeland Security (DHS), sector-specific agencies, or private-sector organizations.[6] In 2009, the Obama Administration established the National Cybersecurity and Communications Integration Center (NCCIC) "to bolster information sharing and incident response" with respect to critical infrastructure in particular.[7]

Legislation focusing specifically on alleviating obstacles to information sharing in cybersecurity were first considered in the 112th Congress.[8] The Cyber Intelligence Sharing and Protection Act (CISPA, H.R. 3523) passed the House in the second session but received no action in the Senate. The Cybersecurity Information Sharing Act (CISA, S. 2102) of 2012 was largely incorporated into the Cybersecurity Act of 2012 (S. 3414), which was debated in the Senate but failed two attempts at cloture. The Obama Administration also proposed legislation during the 112th Congress that included provisions on information sharing.[9]

CISPA was reintroduced with little change in the 113th Congress as H.R. 624. An amended version passed the House but once again received no action in the Senate. A substantially amended version of CISA was reintroduced and reported in the Senate (S. 2588) but also received no further action. However, a bill authorizing NCCIC was enacted (S. 2519, P.L. 113-282),[10] along with four other cybersecurity bills with provisions on the protection of critical

[3] See, for example, Sara Sorcher, "Security Pros: Cyberthreat Info-Sharing Won't Be as Effective as Congress Thinks," *Christian Science Monitor*, June 12, 2015, http://www.csmonitor.com/World/Passcode/2015/0612/Security-pros-Cyberthreat-info-sharing-won-t-be-as-effective-as-Congress-thinks.

[4] Notable examples include the chemical industry, electricity, financial, and transportation sectors.

[5] ISACs were originally formed pursuant to a 1998 presidential directive (The White House, "Presidential Decision Directive 63: Critical Infrastructure Protection," May 22, 1998, http://www.fas.org/irp/offdocs/pdd/pdd-63.htm).

[6] See also CRS Report R42114, *Federal Laws Relating to Cybersecurity: Overview of Major Issues, Current Laws, and Proposed Legislation*, by Eric A. Fischer; CRS Report R42984, *The 2013 Cybersecurity Executive Order: Overview and Considerations for Congress*, by Eric A. Fischer et al.; CRS Report R43821, *Legislation to Facilitate Cybersecurity Information Sharing: Economic Analysis*, by N. Eric Weiss.

[7] Department of Homeland Security, "Secretary Napolitano Opens New National Cybersecurity and Communications Integration Center," Press Release, October 30, 2009, http://www.dhs.gov/ynews/releases/pr_1256914923094.shtm.

[8] Some bills in earlier Congresses had addressed aspects of information sharing. For example, H.R. 5548 and S. 3480 in the 111th Congress included some provisions on bidirectional information sharing between the federal government and nonfederal entities.

[9] The White House, "Department of Homeland Security Cybersecurity Authority and Information Sharing," May 12, 2011, http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/dhs-cybersecurity-authority.pdf.

[10] H.R. 3696, the National Cybersecurity and Critical Infrastructure Protection Act, would also have authorized the NCCIC. It passed the House but received no further action in the Senate.

infrastructure and federal information systems, research and development, and the cybersecurity workforce.[11]

Current Legislative Proposals

House Consideration of NCPAA and PCNA

PCNA (H.R. 1560) was introduced March 24, 2015, and reported by the House Intelligence Committee on April 13 (H.Rept. 114-63). NCPAA (H.R. 1731) was introduced April 13 and reported by the House Homeland Security Committee on April 17 (H.Rept. 114-83). The House Committee on Rules held a hearing on proposed amendments to both bills on April 21. More than 30 amendments were submitted for NCPAA and more than 20 for PCNA.[12] The committee reported H.Res. 212 (H.Rept. 114-88) on the two bills on April 21, with a structured rule allowing consideration of five amendments to PCNA and 11 for NCPAA. For each bill, a manager's amendment would serve as the base bill for floor consideration, with debate on PCNA held on April 22 and on NCPAA on April 23. The rule further stated that upon passage of both bills, the text of H.R. 1731 would be appended to H.R. 1560, and H.R. 1731 would be tabled.

On April 22, all five amendments to H.R. 1560 were adopted and the bill passed the House by a vote of 307 to 116. The amendments were all agreed to by voice vote except a sunset amendment terminating the bill's provisions seven years after enactment, which passed by recorded vote of 313 to 110. Similarly, on April 23, the 11 amendments to H.R. 1731 were all adopted and the bill was passed by a vote of 355 to 63. A sunset amendment similar to that approved for H.R. 1560 and all but one other amendment were adopted by voice vote. The exception, requiring a GAO study on privacy and civil liberties impacts, was agreed to by recorded vote, 405 to 8. The engrossed version of H.R. 1560 combined the bills by making PCNA Title I and NCPAA Title II.[13]

Senate Consideration of CISA

CISA was introduced and reported by the Senate Intelligence Committee on March 17, 2015, with a written report filed April 15 (S.Rept. 114-32). The bill was offered as an amendment to H.R. 1735, the National Defense Authorization Act for 2016 (NDAA), but a cloture vote on the amendment failed on June 11. A motion to proceed on CISA was filed on August 3, along with a cloture motion. More than 70 amendments to the bill were filed. The cloture motion was withdrawn on August 5 after a unanimous consent agreement was reached permitting consideration, and the Senate began debate on a manager's amendment on October 20. The substitute included several of the filed amendments. Several additional amendments were considered, but most did not succeed. The Senate passed CISA, as amended, on October 27.

[11] See CRS Report R43831, *Cybersecurity Issues and Challenges: In Brief*, by Eric A. Fischer

[12] For a list of amendments and text, see House Committee on Rules, "H.R. 1731—National Cybersecurity Protection Advancement Act of 2015," April 21, 2015, http://rules.house.gov/bill/114/hr-1731, and "H.R. 1560—Protecting Cyber Networks Act," April 21, 2015, http://rules.house.gov/bill/114/hr-1560.

[13] To avoid confusion about the passed and engrossed versions of H.R. 1560, the two bills are referred to hereinafter by their names, not their original bill numbers. CISA will also be referred to by name rather than bill number.

Other Legislative Proposals in the 114th Congress

Two other bills on information sharing have been introduced in the 114th Congress, one in the House and one in the Senate. The White House has also submitted a legislative proposal[14] (WHP) and issued an executive order on the topic.[15] The other bills are

- the Cyber Intelligence Sharing and Protection Act (CISPA), which passed the House in the 113th Congress and was reintroduced unamended as H.R. 234; and
- the Cyber Threat Sharing Act of 2015, S. 456, which is similar to the WHP.[16]

Overview of the Legislative Proposals

All the bills would address common concerns about barriers to sharing of information on threats, attacks, vulnerabilities, and other aspects of cybersecurity—both within and across sectors—but they vary somewhat in emphasis and method. NCPAA focuses on the role of the Department of Homeland Security (DHS), and in particular the National Cybersecurity and Communications Integration Center (NCCIC), the role of which is also addressed in S. 456 and the WHP.

PCNA, in contrast, focuses more on the role of the intelligence community (IC),[17] including explicit authorization of the Cyber Threat Intelligence Integration Center (CTIIC), the establishment of which was announced by the Obama Administration in February 2015.[18] Similar authorizing language was included in H.R. 2596, the Intelligence Authorization Act for Fiscal Year 2016, which passed the House June 16. The White House announced opposition to the provisions in the bill on CTIIC's mission and personnel, arguing that they would interfere with the functions of the center as envisioned by the Administration.[19] Both CISPA and CISA address roles of DHS and the IC but do not specifically reference the NCCIC or CTIIC.

All five bills and the WHP have provisions aimed at facilitating sharing of information among private-sector entities and providing protections from liability that might arise from such sharing.[20] They vary somewhat in the kinds of private-sector entities and information covered. In general, the proposals limit the use of shared information to purposes of cybersecurity and specified aspects of law enforcement, and they limit government use for regulatory purposes.

---

[14] The White House, *Updated Information Sharing Legislative Proposal*, 2015, http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/updated-information-sharing-legislative-proposal.pdf.

[15] Executive Order 13691, "Promoting Private Sector Cybersecurity Information Sharing," *Federal Register* 80, no. 34, February 20, 2015, pp. 9349–9353, http://www.gpo.gov/fdsys/pkg/FR-2015-02-20/pdf/2015-03714.pdf.

[16] See Senate Committee on Homeland Security and Governmental Affairs, *Protecting America from Cyber Attacks: The Importance of Information Sharing*, 2015, http://www.hsgac.senate.gov/hearings/protecting-america-from-cyber-attacks-the-importance-of-information-sharing. The hearing was not specifically on the White House proposal but it was held after the proposal was submitted and before the introduction of S. 456.

[17] The IC consists of 17 agencies and others as designated under 50 U.S.C. 3003.

[18] The White House, "Fact Sheet: Cyber Threat Intelligence Integration Center," press release, February 25, 2015, https://www.whitehouse.gov/the-press-office/2015/02/25/fact-sheet-cyber-threat-intelligence-integration-center.

[19] Office of Management and Budget, "H.R. 2596—Intelligence Authorization Act for FY 2016" (Statement of Administration Policy, June 15, 2015), https://www.whitehouse.gov/sites/default/files/omb/legislative/sap/114/saphr2596r_20150615.pdf.

[20] The House-passed version of H.R. 1735, the National Defense Authorization Act for Fiscal Year 2016, contains provisions protecting certain classes of contractors from liability for information sharing, but the Senate-passed version does not contain those provisions.

NCPAA, PCNA, and CISA would explicitly authorize private-sector entities to monitor and use defensive measures to protect their own systems and those of other consenting entities. CISPA does not directly authorize those actions, but its provisions appear to cover monitoring.[21] S. 456 and the WHP do not cover monitoring or defense.

All address concerns about privacy and civil liberties, although the mechanisms proposed vary to some extent, in particular the roles played by the Attorney General, the Secretary of Homeland Security, Chief Privacy Officers, the Privacy and Civil Liberties Oversight Board (PCLOB), and the Inspectors General of DHS and other agencies. All the proposals require reports to Congress on impacts of their provisions. All also include provisions to shield information shared with the federal government from public disclosure, including exemption from disclosure under the Freedom of Information Act (FOIA).

In addition, NCPAA, S. 456, and the WHP address and modify the roles of information sharing and analysis organizations (ISAOs).[22] ISAOs were defined in the Homeland Security Act (HSA, 6 U.S.C. §131(5)) as entities that gather and analyze information relating to the security of critical infrastructure, communicate such information to help with defense against and recovery from incidents, and disseminate such information to any entities that might assist in carrying out those goals. Information Sharing and Analysis Centers (ISACs) are more familiar to most observers. They may arguably be ISAOs under the definition in HSA but have a different origin, having been formed pursuant to a 1998 presidential directive.[23]

Executive Order 13691,[24] issued soon after the WHP, also addresses the role of ISAOs. It requires the Secretary of Homeland Security to encourage and facilitate the formation of ISAOs, and to choose and work with a nongovernmental standards organization to identify standards and guidelines for them.[25] It also requires the NCCIC to coordinate with ISAOs on information sharing, and includes some provisions to facilitate sharing of classified cybersecurity information with appropriate entities.

NCPAA and CISA also contain provisions relating to cybersecurity of federal agencies and their information systems and of critical infrastructure sectors. CISA also has provisions on international cybersecurity policy and cybercrime.

---

[21] It permits covered entities to "use cybersecurity systems to identify and obtain cyber threat information to protect the rights and property" of covered entities (Sec. 3(a), modifying Sec. 1104(b) of the National Security Act).

[22] The House Committee on Homeland Security held two hearings on the White House proposal before H.R. 1731 was introduced (House Committee on Homeland Security, *Examining the President's Cybersecurity Information Sharing Proposal*, 2015, http://homeland.house.gov/hearing/hearing-administration-s-cybersecurity-legislative-proposal-information-sharing; House Committee on Homeland Security, Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies, *Industry Perspectives on the President's Cybersecurity Information Sharing Proposal*, 2015, http://homeland.house.gov/hearing/subcommittee-hearing-industry-perspectives-president-s-cybersecurity-information-sharing).

[23] The White House, "Presidential Decision Directive 63: Critical Infrastructure Protection," May 22, 1998, http://www.fas.org/irp/offdocs/pdd/pdd-63.htm. The directive envisioned a single center for analysis and sharing of private-sector information relating to the protection of critical infrastructure, with specific design and functions determined by the private sector, in consultation with the federal government. That consultation resulted in the establishment of sector-specific ISACs, with the first, covering the financial sector, established in 1999 (ISAC Council, "Reach of the Major ISACs," January 31, 2004, http://www.isaccouncil.org/images/Reach_of_the_Major_ISACs_013104.pdf).

[24] Executive Order 13691, "Promoting Private Sector Cybersecurity Information Sharing."

[25] DHS has posted a Notice of Funding Opportunity for the standards organization, with selection expected in August 2015 (see Department of Homeland Security, "Information Sharing and Analysis Organizations," May 27, 2015, http://www.dhs.gov/isao).

On April 21, the White House announced support for passage of both NCPAA and PCNA by the House, while calling for a narrowing of sweep for the liability protections and additional safeguards relating to use of defensive measures in both bills.[26] It also called for clarifying provisions in NCPAA on use of shared information in federal law enforcement and ensuring that provisions in PCNA do not interfere with privacy and civil liberties protections. As described above, the White House has also expressed opposition to the provisions on the mission and personnel of CTIIC in PCNA. The Department of Homeland Security raised concerns about some of the provisions in the reported version of CISA in July 2015.[27] On October 22, the White House announced support for passage by the Senate of CISA as amended, while expressing some concerns, in particular about provisions on the use of defensive measures.[28]

Selected Issues

Several issues appear to be particularly relevant to the debate over information-sharing legislation. Among them are the following:

- **Kinds of Information.** What are the kinds of information for which barriers to sharing exist that make effective cybersecurity more difficult, and what are those barriers?
- **Information-Sharing Process.** How should the gathering and sharing of information be structured in the public and private sectors to ensure that it is efficient, effective, and appropriate?
- **Uses of Information.** What limitations should be placed on how shared information is used?
- **Standards and Practices.** What improvements to current standards and practices are needed to ensure that information sharing is useful and efficient for protecting information systems, networks, and their contents?
- **Privacy and Civil Liberties.** What are the risks to privacy rights and civil liberties of individual citizens associated with sharing different kinds of cybersecurity information, and how can those rights and liberties best be protected?
- **Liability Protections.** What, if any, statutory protections against liability are needed to reduce disincentives for private-sector entities to share cybersecurity information with each other and with government agencies, and how can the need to reduce such barriers best be balanced against any risks to well-established protections?

[26] Office of Management and Budget, "H.R. 1560—Protecting Cyber Networks Act," Statement of Administration Policy, April 21, 2015, https://www.whitehouse.gov/sites/default/files/omb/legislative/sap/114/saphr1560r_20150421.pdf; Office of Management and Budget, "H.R. 1731—National Cybersecurity Protection Advancement Act of 2015," Statement of Administration Policy, April 21, 2015, https://www.whitehouse.gov/sites/default/files/omb/legislative/sap/114/saphr1731r_20150421.pdf.

[27] Alejandro N. Mayorkas, "Letter to Senator Al Franken," July 31, 2015, http://www.franken.senate.gov/files/documents/150731DHSresponse.pdf.

[28] Office of Management and Budget, "S. 754—Cybersecurity Information Sharing Act of 2015" (Statement of Administration Policy, October 22, 2015), https://www.whitehouse.gov/sites/default/files/omb/legislative/sap/114/saps754s_20151022.pdf.

An in-depth discussion of these issues is beyond the scope of this report. However, the points described below may be relevant for congressional debate. For discussion of legal issues associated with privacy, civil liberties, and liability protections, see CRS Report R43941, *Cybersecurity and Information Sharing: Legal Challenges and Solutions*, by Andrew Nolan.

Information that may be usefully shared can be complex in type and purpose, which may complicate determining the best methods and criteria for sharing. Information sharing can involve a broad variety of material communicated on a wide range of timescales, from broad cybersecurity policies and principles to best practices to information on threat intelligence,[29] vulnerabilities, and defenses to computer-generated data transmitted directly from one information system to another electronically. The level of sensitivity of information can also vary—for example, it may be classified, proprietary, or personal. Information of any class will also vary in its value for cybersecurity and the degree to which it needs human processing to be useful.[30]

Shared information can be used for a variety of purposes relating to cybersecurity. A widely recognized objective is to inform situational awareness—an understanding of the components, operational roles, and current and projected states of systems and networks being protected; events occurring within and across them; and threats, vulnerabilities, and other elements of risk, all in the context of the larger cyberspace environment. Shared information may also be used for identifying specific defensive actions or measures, and for planning and capacity-building, among other objectives.[31] In addition, the same information may have different utility for different users—for example, threat signatures relating to attacks on one critical infrastructure sector may be of marginal concern for another, and best practices may be much more useful for small businesses than signatures associated with advanced targeted threats. Also, shared information may prove of little use if it is delayed, provided without relevant contextual detail, or provided in a form that requires substantial additional processing to determine its applicability. If recipients find that the information they are provided is of little use to them, they may be less likely to participate in or continue with information-sharing initiatives.

The timescale during which shared information will be most useful varies with the kind of information shared and its purpose. To the extent that the goal of information sharing is to defend systems and networks against cyberattacks, there appears to be a consensus that shared information needs to be actionable—that is, it should identify or evoke a specific response aimed at mitigating cybersecurity risks. To be meaningfully actionable, information may often need to be shared very quickly or even in an automated fashion. Such rapid communication, for example by machine-to-machine transmission and processing, is sometimes called "real-time" or "near real-time" sharing. The relevance of timing for shared information may be measured in seconds

[29] This can be described as "indicators (i.e., an artifact or observable that suggests that an attack is imminent, that an attack is underway, or that a compromise may have already occurred); the TTPs [tactics, techniques, and procedures] of an adversary; and recommended actions to counter an attack" (Chris Johnson, Lee Badger, and David Waltermire, *Guide to Cyber Threat Information Sharing (Draft)*, SP 800-150, National Institute of Standards and Technology, October 2014, 4, http://csrc.nist.gov/publications/drafts/800-150/sp800_150_draft.pdf).

[30] See, for example, Kathleen M. Moriarty, "Transforming Expectations for Threat-Intelligence Sharing," *RSA Perspective*, August 3, 2013, https://www.emc.com/collateral/emc-perspective/h12175-transf-expect-for-threat-intell-sharing.pdf.

[31] See, for example, Department of Homeland Security, "Information Sharing: A Vital Resource," March 10, 2015, http://www.dhs.gov/information-sharing-vital-resource; Robin M. Ruefle and M. Murray, "CSIRT Requirements for Situational Awareness," Carnegie Mellon University, January 25, 2014, http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA596848.

or even milliseconds in many cases.[32] There may be little or no time for human operators to examine a specific parcel of data to determine whether sharing it could raise privacy, liability, or other concerns. Therefore, the way that such sharing is implemented may affect not only operational effectiveness, but also other interests and goals such as privacy.

A large increase in information sharing could potentially lead to information overload, reducing the effectiveness of the sharing in reducing cybersecurity risks. The relationship between the volume of information shared and improved cybersecurity is not straightforward. Given the broad classes of information that might be candidates for sharing, and the sheer volume of available data, an entity could receive much more information than it can reasonably process with available resources. Both providers and recipients—whether they are businesses, ISACs, ISAOs, or government agencies—will incur various costs, including developing, assessing, processing, sharing, and applying the information. For sharing to be effective, information from the provider must be relevant to recipients' needs and in forms that can be readily applied in their information technology and security environments. Recipients must also have the capacity and willingness to assess and use the information received in a timely fashion. A large increase in the amount of information received may be counterproductive, especially if much of the information proves to be of little use to the recipient. That could include not only information of uncertain quality and use, but also similar or redundant information from a variety of sources, which could lead to misdirection and waste of resources and could result in important information being overlooked. However, determining a priori what information is useful to share may be difficult.[33]

The current structure for information sharing is fairly complex but arguably limited in scope. Several federal entities in addition to NCCIC and CTIIC are involved. For example, the National Cyber Investigative Joint Task Force (NCIJTF), which is operated by the Federal Bureau of Investigation (FBI), shares information on investigations related to domestic cyberthreats with national security and criminal law-enforcement programs.[34] Other entities with broader missions may also be involved in cybersecurity information sharing—for example, the federal Information Sharing Environment,[35] and state and local fusion centers.[36] There are also many private-sector entities with information-sharing missions, most notably the ISACs, of which 19 are members of the national council.[37]

Currently, there appear to be two general models for information sharing—a decentralized, "peer-to-peer," often informal approach between entities with complementary needs, and a more centralized "hub-and-spoke" model such as the ISACs.[38] Organizations such as ISACs are generally sector-specific. Not all sectors have such organizations, and affiliations other than

[32] See, for example, M.J. Herring and K.D. Willett, "Active Cyber Defense: A Vision for Real-Time Cyber Defense," *Journal of Information Warfare* 13, no. 2, April 2014, pp. 46–55, https://www.nsa.gov/ia/_files/JIW-13-2—23-April-2014—Final-Version.pdf.

[33] See, for example, Moriarty, "Transforming Expectations for Threat-Intelligence Sharing."

[34] Federal Bureau of Investigation, "National Cyber Investigative Joint Task Force," 2015, http://www.fbi.gov/about-us/investigate/cyber/ncijtf.

[35] Information Sharing and Access Interagency Policy Committee, "Information Sharing Environment (ISE)," 2015, http://www.ise.gov/.

[36] National Fusion Center Association, "National Strategy for the National Network of Fusion Centers, 2014-2017," July 2014, https://nfcausa.org/html/National%20Strategy%20for%20the%20National%20Network%20of%20Fusion%20Centers.pdf.

[37] National Council of ISACs, "Member ISACs," 2015, http://www.isaccouncil.org/memberisacs.html.

[38] Denise E. Zheng and James A. Lewis, *Cyber Threat Information Sharing: Recommendations for Congress and the Administration*, CSIS, March 2015, https://csis.org/files/publication/150310_cyberthreatinfosharing.pdf.

sector may also be important for some kinds of information sharing. Filling such gaps appears to be part of the rationale behind the Administration's ISAO proposal to broaden the scope of ISAOs beyond that described in the Homeland Security Act.[39] On the one hand, the absence of an appropriate mechanism can be a barrier to information sharing for an entity. On the other hand, a proliferation of mechanisms, such as some observers fear the Administration's ISAO model might result in, could also serve as a barrier if it makes information sharing inefficient or confusing for possible participants.

A proliferation of sharing mechanisms could improve coverage for information sharing among sectors but might also lead to duplication or overspecialization. Those could lead to a reduction in effective sharing across sectors, for example, and lack of clarity with respect to responsibilities. It also creates the possibility that entities could receive conflicting information or even incompatible recommendations from different sharing organizations. However, the potential for duplication creates the potential for market competition, and such market forces would ideally yield more innovation and more rapid improvement in information sharing than would a more restricted approach. Market forces might also lead to lower costs, and cost can be an impediment to improved information sharing, especially for small businesses. Yet market forces might also lead to higher costs, and a proliferation of sharing mechanisms might also make decisions about which one or ones to join more difficult for potential participants. In contrast, a narrow, tightly defined structure for information sharing could lead to logjams or impede innovation in response to the continuing evolution of cyberspace.

Development of consensus standards and best practices may improve the effectiveness and efficiency of information sharing.[40] The adoption of standards for information sharing is one way to help address concerns about reliability and utility of information received. Such an effort may be especially useful if the number and scope of ISAOs grows significantly, as may be the case under the Obama Administration proposal and EO 13691. Dozens of standards currently exist relating to information sharing.[41] The Department of Homeland Security has been developing a single set applicable to sharing of threat intelligence.[42] However, the large variation in sharing requirements and benefits among different entities and sectors may pose a significant challenge to the development of a useful common set of standards and practices. Nevertheless, experience with the development of the NIST cybersecurity framework suggests that it may be possible to create a sufficiently flexible structure that entities can use to identify and develop appropriate standards and practices.[43]

Protection of confidentiality, privacy, and civil liberties in information sharing remains an area of controversy. Concerns relating to privacy and civil liberties, especially the protection of personal and proprietary information and uses of shared information, have been a subject of considerable

[39] The White House, *Updated Information Sharing Legislative Proposal*; The White House, "Fact Sheet: Executive Order Promoting Private Sector Cybersecurity Information Sharing" (Press Release, February 12, 2015), http://www.whitehouse.gov/the-press-office/2015/02/12/fact-sheet-executive-order-promoting-private-sector-cybersecurity-inform; Executive Order 13691, "Promoting Private Sector Cybersecurity Information Sharing."

[40] See, for example, Moriarty, "Transforming Expectations for Threat-Intelligence Sharing."

[41] European Union Agency for Network and Information Security, *Standards and Tools for Exchange and Processing of Actionable Information*, November 2014, https://www.enisa.europa.eu/activities/cert/support/actionable-information/standards-and-tools-for-exchange-and-processing-of-actionable-information.

[42] Department of Homeland Security, "Information Sharing Specifications for Cybersecurity," 2015, https://www.us-cert.gov/Information-Sharing-Specifications-Cybersecurity.

[43] See CRS Report R42984, *The 2013 Cybersecurity Executive Order: Overview and Considerations for Congress*, by Eric A. Fischer et al.

debate in the development of legislation on information sharing. The bills contain provisions aimed at reducing risks of inappropriate sharing and use of such information. Observers vary significantly in assessments about the adequacy of those safeguards, both in general and with respect to the House and Senate bills.[44] Some observers argue that shared cybersecurity information seldom needs to include privacy-related information,[45] which suggests that privacy concerns may be limited and comparatively easy to address. However, the issue is complicated by various factors, including potential impacts of advances in data analytic capabilities, often referred to as "big data." According to a presidential advisory panel, "By data mining and other kinds of analytics, nonobvious and sometimes private information can be derived from data that, at the time of their collection, seemed to raise no, or only manageable, privacy issues."[46] There are many potential sources, unrelated to the information-sharing activities addressed in the bills, from which an individual's personal information in cyberspace can be identified and acquired by various entities. The impacts of data mining and analytics do not appear to have generally been analyzed with respect to the potential risks to confidentiality and privacy of private- and public-sector information-sharing activities in comparison to risks from other kinds of activities.

Sharing of information among private-sector entities might not be substantially increased by the actions contemplated in the legislation. Most observers appear to believe that legislation on information sharing is either necessary or at least potentially beneficial—provided that appropriate protections are included. Some observers have noted that the benefits of receiving cybersecurity information tend to outweigh the benefits of providing such information for many organizations.[47] This may be especially true for information shared with the federal government.[48] Timely and actionable information that an entity receives can help it prevent or mitigate an attack. In the absence of incentives for reciprocity, however, it is hard to see what benefit an organization would gain from providing information, unless it is a government entity whose mission is to provide such data or a provider of cybersecurity services. More indirect benefits might occur, for example, if a pattern of reciprocity develops among sharing entities, such as through ISACs or ISAOs. However, information sharing by itself is not sufficient to improve cybersecurity. Not only must the information be actionable, but the recipient must also have processes, including equipment and software, in place to use the information effectively. If such processes are not in

[44] See, for example, Dean C. Garfield, President and CEO, Information Technology Industry Council, "Letter to Sens. Mitch McConnell and Harry Reid," July 23, 2015, http://www.itic.org/policy/ITICISASenateLetter07-23-2015.pdf; Robyn Greene, "Is CISA Gift-Wrapped for Hackers and Nation-State Actors?," *The Hill*, August 3, 2015, http://thehill.com/blogs/pundits-blog/technology/250070-is-cisa-gift-wrapped-for-hackers-and-nation-state-actors; House Committee on Homeland Security, Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies, *Industry Perspectives on the President's Cybersecurity Information Sharing Proposal*; Mayorkas, "Letter to Senator Al Franken"; Office of Management and Budget, "H.R. 1560—Protecting Cyber Networks Act"; Office of Management and Budget, "H.R. 1731—National Cybersecurity Protection Advancement Act of 2015."

[45] See, for example, David Inserra and Paul Rosenzweig, "Cybersecurity Information Sharing: One Step Toward U.S. Security, Prosperity, and Freedom in Cyberspace," Backgrounder #2899 (The Heritage Foundation, April 1, 2014); Kimberley Peretti, "Cyber Threat Intelligence: To Share or Not to Share—What Are the Real Concerns?," *Privacy and Security Law Report* 13, no. 1476 (September 1, 2014), http://www.alston.com/Files/Publication/09a5e602-0f0c-4635-b5eb-685811791486/Presentation/PublicationAttachment/629e5e52-4200-422a-a3e1-6fa39e6b2ff5/Bloomberg%20BNA_KPeretti_LDennig_Cyber%20Threat%20Intel%208%2029%2014.pdf.

[46] President's Council of Advisors on Science and Technology, "Big Data and Privacy: A Technological Perspective," April 30, 2014, p. ix, https://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf.

[47] See, for example, CRS Report R43821, *Legislation to Facilitate Cybersecurity Information Sharing: Economic Analysis*, by N. Eric Weiss; Zheng and Lewis, "Cyber Threat Information Sharing: Recommendations for Congress and the Administration."

[48] Sorcher, "Security Pros."

place and utilized properly, the net effect may be the same as if the information were not shared at all.[49]

In addition to issues such as legal concerns that may be associated with providing information, businesses may be concerned about reputation costs, if they provide information showing that they have been victims of cyberattacks. Government measures such as requirements for data-breach notification, as enacted in most states, can provide incentives for organizations to share information that may be useful in attempts to prevent future attacks on other entities or to capture and prosecute cybercriminals. While the legislative proposals on information sharing may reduce the risks to private-sector entities associated with providing information, none include explicit incentives to stimulate such provision. In the absence of mechanisms to balance the asymmetry between incentives for receiving and providing information, the degree to which information sharing would increase under the provisions of the various legislative proposals may be uncertain.

Information sharing is only one facet of cybersecurity.[50] Information sharing is only one of many cybersecurity tools, and some observers have expressed concern about risks associated with an overemphasis on its role in cybersecurity. Sharing may be relatively unimportant for many organizations, especially in comparison with other cybersecurity needs.[51] Entities must also have the resources and processes in place that are necessary for effective cybersecurity risk management. For example, in the data breaches of information on federal employees revealed in June by the Office of Personnel Management (OPM), it is not clear that specific information about the threat or even defensive measures would have resulted in effective defense against the attacks, given OPM's reported shortcomings in implementation of requirements in the Federal Information Security Management Act (FISMA).[52]

In addition, information sharing tends to focus on immediate concerns such as cyberattacks and imminent threats. While those must be addressed, that does not diminish the importance of other issues in cybersecurity such as education and training, workforce, acquisition, or cybercrime law, or major long-term challenges such as building security into the design of hardware and software, changing the incentive structure for cybersecurity, developing a broad consensus about cybersecurity needs and requirements, and adapting to the rapid evolution of cyberspace.

Side-by-Side Comparison of NCPAA, PCNA, and CISA

The remainder of the report consists of four tables comparing provisions in NCPAA and PCNA as passed by the House and CISA as passed by the Senate:

[49] See, for example, Johnson, Badger, and Waltermire, "Guide to Cyber Threat Information Sharing (Draft)."

[50] See, for example, Testimony of Martin C. Libicki before the House Committee on Oversight and Government Reform, Subcommittee on Information Technology, hearing on *Industry Perspectives on the President's Cybersecurity Information Sharing Proposal*, 2015, http://homeland.house.gov/hearing/subcommittee-hearing-industry-perspectives-president-s-cybersecurity-information-sharing.

[51] For example, in the Cybersecurity Framework developed by the National Institute of Standards and Technology, target levels of information sharing vary among the four tiers of cybersecurity implementation developed for organizations with different risk profiles (National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0*, February 12, 2014, http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf).

[52] See, for example, House Committee on Oversight and Government Reform, *OPM: Data Breach*, hearing, June 16, 2015, https://oversight.house.gov/hearing/opm-data-breach; CRS Report R44111, *Cyber Intrusion into U.S. Office of Personnel Management: In Brief*, coordinated by Kristin Finklea

Table 1 provides a side-by-side comparison of sections with corresponding provisions in the three bills and includes all the provisions specifically related to information sharing. The other three tables provide summaries of sections in NCPAA and CISA for which CRS did not identify any corresponding provisions in either of the other bills:

- **Table 2,** on cybersecurity of federal agencies and systems,
- **Table 3,** on critical infrastructure cybersecurity, and
- **Table 4,** on other cybersecurity matters.

However, some sections in those tables are related to sections in **Table 1**. For example, Sec. 203 of CISA is included in **Table 1** rather than **Table 2** because some of its provisions correspond to provisions in Sec. 216 of NCPAA, on the protection of federal information systems. However, Sec. 204 of CISA, on advanced cybersecurity defenses for federal agencies, is in **Table 2**, even though it relates to cybersecurity for federal systems, because there are no comparable provisions in either NCPAA or PCNA. In contrast, Sec. 204 of NCPAA, on ISAOs, is in **Table 1** because it is on information sharing, even though there are no corresponding provisions in the other bills. Note that subsections that address topics not found in other bills are included in **Table 1** if other parts of the section have corresponding provisions in other bills. For example, Sec. 104(c) in PCNA, establishing the CTIIC (see p. 27), has no corresponding provisions in the other bills but is included in **Table 1** because the other subsections have corresponding provisions.

Glossary of Abbreviations in the Tables

AG	Attorney General
CI	Critical Infrastructure
CPO	Chief Privacy Officer
CRADA	Cooperative research and development agreement
CTIIC	Cyber Threat Intelligence Integration Center
DHS	Department of Homeland Security
DNI	Director of National Intelligence
DOD	Department of Defense
DOJ	Department of Justice
FIPPs	Fair Information Practice Principles
FISMA	Federal Information Security Modernization Act (44 U.S.C. Chapter 34, subchapter II)
GAO	Government Accountability Office
HHS	Health and Human Services
HSA	Homeland Security Act
HSC	House Committee on Homeland Security
HSGAC	Senate Homeland Security and Governmental Affairs Committee
IC	Intelligence community
ICS	Industrial control system
ICS-CERT	Industrial Control System Cyber Emergency Response Team
IG	Inspector General
ISAC	Information sharing and analysis center

ISAO	Information sharing and analysis organization
MOU	Memorandum of understanding
NCCIC	National Cybersecurity and Communications Integration Center
NCPAA	National Cybersecurity Protection Advancement Act of 2015
NICE	National Initiative for Cybersecurity Education
NIST	National Institute of Standards and Technology
NSS	National Security System(s)
ODNI	Office of the Director of National Intelligence
OMB	Office of Management and Budget
OPM	Office of Personnel Management
PCLOB	Privacy and Civil Liberties Oversight Board
PCNA	Protecting Cyber Networks Act
R&D	Research and development
SSA	Sector-specific agency
Secretary	Secretary of Homeland Security
US-CERT	United States Computer Emergency Readiness Team
U/S-CIP	DHS Under Secretary for Cybersecurity and Infrastructure Protection

Notes on the Tables

Entries describing provisions in a bill are summaries or paraphrases, with direct quotes enclosed in double quotation marks. The tables use the following formatting conventions to aid in the comparison:

- In **Table 1**, related provisions in the bills are adjacent to each other, with NCPAA serving as the basis for comparison.[53] As a result, many provisions of PCNA and CISA appear out of sequence in that table.
- **Bold** formatting denotes that the identified provision is the subject of the subsequent text (e.g., **(d)** or **Sec. 102 (a)**).
- Numbers and names of sections, subsections, and paragraphs (except definitions) added to existing laws by the bills are enclosed in single quotation marks (e.g., **'Sec. 111(a)'**).
- Underlined text (visible only in the pdf version) is used in selected cases in **Table 1** as a visual aid to highlight differences with a corresponding provision in the other bills that might otherwise be difficult to discern.
- The names of titles, sections, and some paragraphs are stated the first time a provision from them is discussed in the tables—for example, **Sec. 103. Authorizations for Preventing, Detecting, Analyzing, and Mitigating Cybersecurity Threats—**but only the number, to the paragraph level or higher, is used thereafter.

[53] This approach was taken for purposes of efficiency and convenience only. CRS does not advocate or take positions on legislation or legislative issues.

- In cases where a provision of a bill is out of sequence from that immediately above it, as much of the provision number is repeated as is needed to make its origin clear. For example, on p. 29, a provision from Sec. 103 of PCNA is described immediately after an entry for Sec. 109 and is therefore labelled **Sec. 103(c)(3)**. That is followed immediately by an entry labelled **(a)**, which is a subsection of Sec. 103 and therefore is not preceded by the section number.
- Page numbers cited within the table are hyperlinked to the provisions they reference in the table; the page numbers themselves refer to pages in the pdf version of this report.
- Explanatory notes on provisions are enclosed in square brackets. Also, the entry "[Similar to {bill}]" means that the text in that provision is closely similar in text, with no significant difference in meaning as interpreted by CRS, to the corresponding provision in the named bill. "[Identical to {bill}]" means that there are no differences in language between the text of that provision and the corresponding provision in the named bill. A double em-dash (——) means that the bill has no provision corresponding to that described for other bills in that row of the table.

See the **"Glossary of Abbreviations in the Tables"** for meanings of abbreviations used therein.

Table 1. Side-by-Side Comparison of Corresponding Sections in PCNA (Title I) and NCPAA (Title II) of H.R. 1560 as Passed by the House and CISA, S. 754, as Passed by the Senate

NCPAA	PCNA	CISA
"To amend the Homeland Security Act of 2002 to enhance multi-directional sharing of information related to cyber-security risks and strengthen privacy and civil liberties protections, and for other purposes."	"To improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes." [*Note:* These two official titles have been concatenated in the engrossed version of H.R. 1560.]	[Identical to PCNA]
		Sec. 1. Table of Contents
		Title I. Cybersecurity Information Sharing
Sec. 201. Short Title	**Sec. 101. Short Title**	**Sec. 101. Short Title**
National Cybersecurity Protection Advancement Act of 2015	Protecting Cyber Networks Act	Cybersecurity Information Sharing Act of 2015
Sec. 202. National Cybersecurity and Communications Integration Center		
Amends Sec. 226 of the HSA (6 U.S.C. 148). [*Note:* This section, added by P.L. 113-282, established the National Cybersecurity and Communications Integration Center and is referred to in the bill as the "second section 226" to distinguish it from an identically numbered section added by P.L. 113-277.]	——	[*Note:* Sec. 203(a) redesignates "second section 226" of the HSA as Sec. 227 and renumbers Sec. 227 and 228 (see p. 53).]
(a) In General	**Sec. 110. Definitions**	**Sec. 102. Definitions**
Amends existing definitions in 6 U.S.C. 148(a):	Defines terms in this title:	Defines terms in this title:
Cybersecurity Risk: Excludes actions solely involving violations of consumer terms of service or licensing agreements from the definition.	——	——
Incident: Replaces the phrase "or constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies" with "or actually or imminently jeopardizes, without lawful authority, an information system."	——	——
Adds the following definitions:		

NCPAA	PCNA	CISA
	Agency: As in 44 U.S.C. 3502.	[Identical to PCNA]
——	——	*Antitrust Laws:* As in 15 U.S.C. 12, 15 U.S.C. 45 as it "applies to unfair methods of competition," and state laws with the same intent and effect.
——	*Appropriate Federal Entities:* Departments of Commerce, Defense, Energy, Homeland Security, Justice, and the Treasury; and Office of the ODNI.	[Identical to PCNA]
——	*Cybersecurity Threat:* An action unprotected by the 1st Amendment to the Constitution that involves an information system and may result in unauthorized efforts to adversely impact the security, integrity, confidentiality, or availability of the system or its contents, but not including actions solely involving violations of consumer terms of service or licensing agreements.	[Similar to PCNA]
Cyber Threat Indicator: Technical information necessary to describe or identify	*Cyber Threat Indicator:* Information or a physical object necessary to describe or identify	*Cyber Threat Indicator:* Information necessary to describe or identify
- a method for "probing, monitoring, maintaining, or establishing network awareness" [defined below] of an information system to discern its technical vulnerabilities, if the method is known or reasonably suspected of association with a known or suspected cybersecurity risk, including	- malicious reconnaissance [*Note:* Definition of this term below includes a method, associated with a known or suspected cybersecurity threat, for probing or monitoring an information system to discern its vulnerabilities], including	[Identical to PCNA]
communications that reasonably appear to have "the purpose of gathering technical information related to a cybersecurity risk,"	anomalous patterns of communications that appear to have "the purpose of gathering technical information related to a cybersecurity threat or security vulnerability,"	[Identical to PCNA]
- a method for defeating a security control or technical control,	- a method of defeating a security control or exploiting a security vulnerability,	[Identical to PCNA]
- "a technical vulnerability including anomalous technical behavior that may become a vulnerability,"	- a security vulnerability or anomalous activity indicating the existence of one,	[Identical to PCNA]

NCPAA	PCNA	CISA
- a method of causing a legitimate user of an information system or its contents to "inadvertently enable the defeat of a technical or operational control,"	- a method of causing a legitimate user of an information system or its contents to unwittingly enable defeat of a security control or exploitation of a security vulnerability,	[Identical to PCNA]
- a method for unauthorized remote identification, access, or use of an information system or its contents, if the method is known or reasonably suspected of association with a known or suspected cybersecurity risk, or	- "malicious cyber command and control," [*Note:* Definition of this term below includes remote identification, access, or use of an information system or its contents.]	[Identical to PCNA]
- actual or potential harm from an incident, including exfiltration of information; or	[Identical to NCPAA]	[Identical to NCPAA]
- any other cybersecurity risk attribute that cannot be used to identify specific persons believed to be unrelated to the risk, and	- any other cybersecurity threat attribute the	[Identical to PCNA]
disclosure of which is not prohibited by law.	disclosure of which is not prohibited by law.	[Identical to PCNA]
- any combination of the above.	——	- "any combination thereof."
Cybersecurity Purpose: Protecting an information system or its contents from a cybersecurity risk or incident or identifying a risk or incident source.	*Cybersecurity Purpose:* Protecting (including by using defensive measures) an information system or its contents from a cybersecurity threat or security vulnerability or identifying a threat source.	*Cybersecurity Purpose:* Protecting an information system or its contents from a cybersecurity threat or security vulnerability.
Defensive Measure: An "action, device, procedure, signature, technique, or other measure applied to an information system" or its contents that "detects, prevents or mitigates a known or suspected cybersecurity risk or incident" or attributes that could help defeat security controls,	*Defensive Measure:* An "action, device, procedure, technique, or other measure" executed on an information system or its contents that "prevents or mitigates a known or suspected cybersecurity threat or security vulnerability."	*Defensive Measure:* An "action, device, procedure, signature, technique, or other measure" applied to an information system that "detects, prevents or mitigates a known or suspected cybersecurity threat or security vulnerability."
but not including "a measure that destroys, renders unusable, or substantially harms an information system" or its contents not operated by that nonfederal entity, except a state, local, or tribal government, or by another nonfederal or federal entity that consented to such actions.	[No Corresponding Provision; however, the authority to operate defensive measures in Sec. 103(b) includes a similar restriction; see p. 31];	but not including "a measure that destroys, renders unusable, provides unauthorized access to, or substantially harms an information system" or its contents not operated by that private entity, or by another [nonfederal] or federal entity that consented to such actions.

NCPAA	PCNA	CISA
——	*Federal Entity:* A U.S. department or agency, or any component thereof.	[Identical to PCNA]
[*Note:* No corresponding provision, but *Information System* is already defined in 6 U.S.C. 148 as 44 U.S.C. 3502.]	*Information System:* As in 44 U.S.C. 3502.	[Identical to PCNA]
——	*Local Government:* A political subdivision of a state.	[Identical to PCNA]
[*Note:* No corresponding provision, but the definition of *Cyber Threat Indicator* includes a method for unauthorized remote identification, access, or use of an information system or its contents, provided that the method is known or reasonably suspected of association with a known or suspected cybersecurity risk.]	*Malicious Cyber Command and Control:* "A method for unauthorized remote identification of, access to, or use of an information system" or its contents.	[Identical to PCNA]
——	*Malicious Reconnaissance:* A method, associated with a known or suspected cybersecurity threat, for probing or monitoring an information system to discern its vulnerabilities.	[Identical to PCNA]
Network Awareness: Scanning, identifying, acquiring, monitoring, logging, or analyzing the contents of an information system.	*Monitor:* Scanning, identifying, acquiring, or otherwise possessing the contents of an information system.	[Identical to PCNA]
[*Note:* Nonfederal government agencies are not expressly defined in the bill but are covered in specific provisions]	*Non-Federal Entity:* A private entity or nonfederal government or agency thereof (including personnel), but not including foreign powers as defined in 50 U.S.C. 1801.	*Entity:* A private entity or nonfederal government or agency thereof, but not including foreign powers as defined in 50 U.S.C. 1801.
Private Entity: A nonfederal entity that is an individual, nonfederal government utility or "an entity performing utility services," or	*Private Entity:* A person, nonfederal government utility, or	*Private Entity:* A person, nonfederal government utility, or
private group, organization, proprietorship, partnership, trust, cooperative, corporation, or other commercial or nonprofit entity,	[Identical to NCPAA]	[Identical to NCPAA]
including personnel.	including personnel, but	[Identical to PCNA]

NCPAA	PCNA	CISA
——	not including a foreign power as defined in 50 U.S.C. 1801.	[Identical to PCNA]
——	*Real Time:* Automated, machine-to-machine system processing of cyber threat indicators where the occurrence and "reporting or recording" of an event are "as simultaneous as technologically and operationally practicable."	——
Security Control: The management, operational, and technical controls used to protect an information system and the information stored on, processed by, or transiting it against unauthorized attempts to adversely affect their confidentiality, integrity, or availability.	*Security Control:* The management, operational, and technical controls used to protect an information system and its information against unauthorized attempts to adversely impact their security, confidentiality, integrity, or availability.	*Security Control:* The management, operational, and technical controls used to protect an information system and its information against unauthorized attempts to adversely affect their confidentiality, integrity, or availability.
——	*Security Vulnerability:* "Any attribute of hardware, software, process, or procedure that could enable or facilitate the defeat of a security control."	[Identical to PCNA]
Sharing: "Providing, receiving, and disseminating."	——	——
——	*Tribal:* As in 25 U.S.C. 450b.	[Identical to PCNA]
(b) Amendment		
Adds tribal governments, private entities, and ISACs as appropriate members of the NCCIC in DHS.	——	——
Sec. 203. Information Sharing Structure and Processes	**Sec. 102. Sharing of Cyber Threat Indicators and Defensive Measures by the Federal Government With Non-federal Entities**	**Sec. 103. Sharing of Information by the Federal Government**
	(a) In General	**(a) In General**
Amends Sec. 226 of the HSA.	Amends Title I of the National Security Act of 1947 by adding a new section.	——
	'Sec. 111. Sharing of Cyber Threat Indicators and Defensive Measures by the Federal Government With Non-Federal Entities'	
	'(a) Sharing by the Federal Government'	

NCPAA	PCNA	CISA
(1) revises the functions of the NCCIC by specifying that it is the "lead" federal civilian interface for information sharing, adding "cyber threat indicators" and "defensive measures" to the subjects it addresses, and expanding its functions to include	**'(1)'** requires the DNI, in consultation with the heads of appropriate federal entities, to develop and promulgate procedures consistent with protection of classified information, intelligence sources and methods, and privacy and civil liberties, for	Requires the DNI, the Secretaries of Homeland Security and Defense, and the AG, in consultation with the heads of appropriate federal entities, to develop and promulgate procedures consistent with protection of classified information, intelligence sources and methods, and privacy and civil liberties, for [*Note:* See also Sec. 105(c), p. 26, requiring DHS to implement the process for sharing electronic threat indicators and defensive measures with the federal government.]
- providing information and recommendations on information sharing,	——	——
- in consultation with other appropriate agencies, collaborating with international partners, including on enhancing "the security and resilience of the global cybersecurity ecosystem," and	——	——
- sharing "cyber threat indicators, defensive measures," and information on cybersecurity risks and incidents with federal and nonfederal entities, including across critical-infrastructure (CI) sectors and with fusion centers. [*Note:* See also the provisions on the CTIIC in PCNA, p. 27.]	timely sharing of classified cyber threat indicators and declassified indicators with relevant nonfederal entities, and sharing of information about imminent or ongoing cybersecurity threats to such entities to prevent and mitigate adverse impacts.	timely sharing of **(1)** classified cyber threat indicators and **(2)** declassified indicators and information with relevant entities, **(4)** sharing of information about cybersecurity threats to such entities to prevent and mitigate adverse impacts, and **(3)** sharing with relevant entities, or the public as appropriate, of unclassified indicators.
——	——	**(5)** periodic sharing of best practices based on federal information, with attention to challenges faced by small businesses.
- notify the Secretary, the HSC, and the HSGAC of significant violations of privacy and civil liberties protections under 'Sec. 226(i)(6),'	——	——
——	**'(2) Development of Procedures'** Requires that procedures for sharing developed by the DNI include methods to notify	**(b) Development of Procedures** **(1)** requires that procedures for sharing developed by the DNI include methods for timely notifying of

NCPAA	PCNA	CISA
- promptly notifying nonfederal entities that have shared information known to be in error or in contravention to section requirements,	nonfederal entities that have received information from a federal entity under the title and known to be in error or in contravention to title requirements or other federal law or policy.	[nonfederal] entities that have received information from a federal entity under the bill and known to be in error or in contravention to requirements in the bill or other federal law or policy, and U.S. persons whose personal information was shared by a federal entity in violation of the bill.
- participating in DHS-run exercises, and	——	——
——	Requires that the procedures incorporate existing information-sharing mechanisms of federal and nonfederal entities, including ISACs, as much as possible, and	[Identical to PCNA]
——	include methods to promote efficient granting of security clearances to appropriate representatives of nonfederal entities.	——
——	——	**(2)** requires that the procedures be developed in coordination with appropriate federal entities, including the Small Business Administration and the National Laboratories, to ensure implementation of timely sharing of indicators. [*Note:* See also PCNA, Sec. 103(f) on small business, p. 22.]
(2) expands NCCIC membership to include the following [*Note:* all are existing entities]:	——	——
- an entity that collaborates with state and local governments on risks and incidents and has a voluntary information sharing relationship with the NCCIC,	——	——
- the US-CERT for collaboratively addressing, responding to, providing technical assistance upon request on, and coordinating information about and timely sharing of threat indicators, defensive measures, analysis, or information about cybersecurity risks and incidents,	——	——
- the ICS-CERT to coordinate with ICS owners and operators, provide training on ICS cybersecurity,	——	——

NCPAA	PCNA	CISA
timely share information about indicators, defensive measures, or cybersecurity risks and incidents of ICS, and remain current on ICS technology advances and best practices,		
- the "National Coordinating Center for Communications to coordinate the protection, response, and recovery of emergency communications," and	——	——
- "an entity that coordinates with small and medium-sized businesses."	——	——
(3) adds "cyber threat indicators" and "defensive measures" to the subjects covered in the principles of operation of the NCCIC,	——	——
	Sec. 103. Authorizations for Preventing, Detecting, Analyzing, and Mitigating Cybersecurity Threats	
	(f) Small Business Participation	
Requires that information be shared as appropriate with small and medium-sized businesses and that the NCCIC make self-assessment tools available to them,	Requires the Small Business Administration to assist small businesses and financial institutions in monitoring, defensive measures, and sharing information under the section.	——
——	Requires a report with recommendations by the administrator to the President within one year of enactment on sharing by those institutions and use of shared information for network defense. Requires federal outreach to those institutions to encourage them to exercise the authorities provided under the section.	——
Specifies that information be guarded against disclosure.	——	——
Stipulates that the NCCIC must work with the DHS CPO to ensure that the NCCIC follows privacy and	——	——

NCPAA	PCNA	CISA
civil liberties policies and procedures under 'Sec. 226(i)(6)';		
(4) adds new subsections to Sec. 226 of the HSA:	——	——
'(g) Rapid Automated Sharing'		
'(1)' requires the DHS U/S-CIP to develop capabilities, in coordination with stakeholders and based as appropriate on existing standards and approaches in the information technology industry, that support and advance automated and timely sharing of threat indicators and defensive measures to and from the NCCIC and with SSAs for each CI sector in accordance with 'Sec. 226(h).'.	**'Sec. 111(a)(2)'** requires that the procedures ensure the capability of real-time sharing consistent with protection of classified information. [*Note:* 'Sec. 111(b)(2)' requires procedures to ensure such sharing—see p. 25.]	**(1)** [Identical to PCNA]
'(2)' requires the U/S-CIP to report to Congress twice per year on the status and progress of that capability until it is fully implemented.	——	——
'(h) Sector Specific Agencies'		
Requires the Secretary to collaborate with relevant CI sectors and heads of appropriate federal agencies to recognize each CI SSA designated as of March 25, 2015, in the DHS National Infrastructure Protection Plan. Designates the Secretary as SSA head for each sector for which DHS is the SSA. Requires the Secretary to coordinate with relevant SSAs to - support CI sector security and resilience activities, - provide knowledge, expertise, and assistance on request, and - support timely sharing of threat indicators and defensive measures with the NCCIC.	——	——
	'(b) Definitions'	
——	Defines the following terms by reference to Sec. 110 of the title: *Appropriate Federal Entities, Cyber Threat Indicator, Defensive Measure, Federal Entity,* and *Non-Federal Entity.*	——

NCPAA	PCNA	CISA
	(b) Submittal to Congress	
——	Requires that the procedures developed by the DNI be submitted to Congress within 90 days of enactment of the title.	**(c)** Requires that the procedures developed by the DNI be submitted to Congress within 60 days of enactment of the bill.
	(c) Table of Contents Amendment	
——	Revises the table of contents of the National Security Act of 1947 to reflect the addition of 'Sec. 111.'	——
	Sec. 104. Sharing of Cyber Threat Indicators and Defensive Measures with Appropriate Federal Entities Other Than the Department of Defense or the National Security Agency	**Sec. 105. Sharing of Cyber Threat Indicators and Defensive Measures with the Federal Government**
	(a) Requirement for Policies and Procedures	**(a) Requirement for Policies and Procedures**
——	(1) Adds new subsections to 'Sec. 111' of the National Security Act of 1947	——
'(i) Voluntary Information Sharing Procedures'	**'(b) Policies and Procedures for Sharing with the Appropriate Federal Entities Other Than the Department of Defense or the National Security Agency'**	
'(1)' permits voluntary information-sharing relationships for cybersecurity purposes between the NCCIC and nonfederal entities but prohibits requiring such an agreement. Permits the NCCIC, at the sole and unreviewable discretion of the Secretary, acting through the U/S-CIP, to terminate an agreement for repeated, intentional violation of the terms of '(i).' Permits the Secretary, solely and unreviewably and acting through the U/S-CIP, to deny an agreement for national security reasons.	**'(1)'** requires the President to develop and submit to Congress policies and procedures for federal receipt of cyber threat indicators and defensive measures.	**(1)** requires the AG and the Secretary, in coordination with heads of appropriate agencies, to develop and submit to Congress policies and procedures for federal receipt of cyber threat indicators and defensive measures.
'(2)' permits the relationship to be established through a standard agreement for nonfederal entities not requiring specific terms. Stipulates negotiated agreements with DHS upon	——	——

NCPAA	PCNA	CISA
request of a nonfederal entity where NCCIC has determined that they are appropriate, and at the sole and unreviewable discretion of the Secretary, acting through the U/S-CIP.		
Stipulates that any agreement in effect prior to enactment of the title will be deemed in compliance with requirements in '(i).' Requires that those agreements include "relevant privacy protections as in effect" under the CRADA for Cybersecurity Information Sharing and Collaboration, as of December 31st 2014." Also stipulates that an agreement is not required for an entity to be in compliance with '(i).'	——	——
——	**'(2)'** requires that the policies and procedures be developed in accordance with the privacy and civil liberties guidelines under Sec. 104(b) of the title, and ensure	**(3)** requires that, consistent with the privacy and civil liberties guidelines under Sec. (b), the policies and procedures ensure
——	- real-time sharing of indicators from nonfederal entities with appropriate federal entities except DOD,	- automated sharing of indicators from any [nonfederal] entity with the federal government through the real-time process under (c),
——	- receipt without delay, modification, or other action except for good cause that could impede receipt, and	- real-time receipt. subject only to delay, modification, or other action that could impede receipt
——	——	due to process controls unanimously agreed upon by appropriate agency heads, carried out before retention or use of the indicators or defensive measures, and uniformly applied to federal entities, with
——	- provision to all relevant federal entities,	- provision permitted to other federal entities, and
——	——	- if not through the process under (c), sharing "as quickly as operationally practicable," without unnecessary delay, and also ensure
——	- audit capability, and	- audit capabilities, and

NCPAA	PCNA	CISA
——	- appropriate sanctions for federal personnel who knowingly and willfully use shared information other than in accordance with the title.	- appropriate sanctions for federal personnel who knowingly and willfully conduct activities under the bill in an unauthorized manner.
——	**(2)** requires that an interim version of the policies and procedures be submitted to Congress within 90 days of enactment of the title, and the final version within 180 days.	**(1)** requires that an interim version of the policies and procedures be submitted to Congress within 60 days of enactment of the title, and **(2)** the final version within 180 days.
——	——	**(4)** requires the AG and Secretary to develop public guidelines on matters appropriate to assist and promote sharing of threat indicators with federal entities, including identification of kinds of information constituting - indicators unlikely to include personal or identifying information, - information protected under privacy laws that is unlikely to be directly related to a threat.
——	——	**(c) Capability and Process Within the Department of Homeland Security**
[*Note:* See also Sec. 203, p. 19, specifying the DHS NCCIC as the lead federal civilian interface for information sharing.]	——	**(1)** requires the Secretary to develop and implement, within 90 days of enactment, a capability and process within DHS that will
——	——	- accept indicators and defensive measures in real time from any entity, and upon certification under (2),
——	——	- be the process for federal receipt of indicators and defensive measures from private entities through electronic means, except for communications about indicators previously shared consistent with Sec. 104 between federal and private entities to describe threats or develop defensive measures, and for communications about cybersecurity threats by a regulated entity with its federal regulatory authority,
——	——	- ensure automated receipt by federal entities of indicators shared in real time with DHS,

NCPAA	PCNA	CISA
——	——	- comply with section policies, procedures, and guidelines,
——	——	- not limit or prohibit otherwise lawful disclosures, including reporting of criminal activity, participating in a federal investigation, and providing indicators or measures under a statutory or contractual requirement.
——	——	**(2)** requires the Secretary, in consultation with the heads of appropriate federal agencies, to certify to Congress at least 10 days before implementation whether the capability and process operates as the process for receipt of indicators and measures from any entity in accordance with section policies, procedures, and guidelines.
——	——	**(3)** requires the Secretary to ensure public notice of and access to the process so that entities may share indicators and measures through it and federal entities receive them in real time.
——	——	**(4)** requires the process under (1) to ensure timely receipt by federal entities of shared indicators and measures.
——	——	**(5)** requires an unclassified report, which may include a classified annex, to Congress by the Secretary within 60 days of enactment on development and implementation of requirements in (1) and (3).
	(c) National Cyber Threat Intelligence Integration Center	
——	**(1)** Adds a new section to the National Security Act of 1947.	——
	'Sec. 119B. Cyber Threat Intelligence Integration Center'	
	'(a) Establishment'	
——	Establishes the CTIIC within the ODNI.	——

NCPAA	PCNA	CISA
	'(b) Director'	
——	Creates a director for the CTIIC, to be appointed by the DNI.	——
	'(c) Primary Missions'	
——	Specifies the missions of the CTIIC with respect to cyberthreat intelligence as - serving as the primary federal organization for analyzing and integrating it, - ensuring full access and support of appropriate agencies to activities and analysis, - disseminating analysis to the President, appropriate agencies, and Congress, - coordinating agency activities, and - conducting strategic federal planning.	——
	'(d) Limitations'	
——	Requires that the CTIIC - have no more than 50 permanent positions, - may not augment staff above that limit in carrying out its primary missions, and - be located in a building owned and operated by an element of the IC,	——
——	**(4)** revises the table of contents of the National Security Act of 1947.	——
'(3) Information Sharing Authorization'	**Sec. 103(c) Authorization for Sharing or Receiving Cyber Threat Indicators or Defensive Measures**	**Sec. 104(c) Authorization for Sharing or Receiving Cyber Threat Indicators or Defensive Measures**
Permits nonfederal entities to share, for cybersecurity purposes, cyber threat indicators, and defensive measures, <u>from their own information systems</u> or those of other entities upon written consent,	**(1)** permits nonfederal entities to share, for cybersecurity purposes <u>and consistent with privacy requirements under (d)(2) and protection of classified information</u>, <u>lawfully obtained</u> cyber threat indicators or defensive measures	**(1)** permits entities to share, "for a cybersecurity purpose <u>and consistent with protection of classified information"</u>, cyber threat indicators or defensive measures
with other nonfederal entities or <u>the NCCIC</u>,	with other nonfederal entities or <u>appropriate federal entities except DOD</u>,	with any [nonfederal] entity or the federal government,

NCPAA	PCNA	CISA
notwithstanding any other provision of law,	notwithstanding any other provision of law,	notwithstanding any other provision of law,
except that nonfederal recipients must comply with lawful restrictions on sharing and use imposed by the source.	**(2)** [Similar to NCPAA]	**(2)** [Similar to NCPAA]
	(d) Protection and Use of Information	**(d) Protection and Use of Information**
Requires reasonable efforts by nonfederal and federal entities, prior to sharing, to	**(2)** requires reasonable efforts by nonfederal entities, before sharing a threat indicator, to	**(2)** requires entities, before sharing a threat indicator, to
safeguard personally identifying information from unintended disclosure or unauthorized access or acquisition and	——	——
remove or exclude such information where it is reasonably believed when it is shared to be unrelated to a cybersecurity risk or incident.	remove information reasonably believed to be personal or identifying of a specific person not directly related to a cybersecurity threat, or implement a technical capability for removing such information.	remove information known to be personal or that identifies a specific person not directly related to a cybersecurity threat, or implement and use a technical capability for removing such information.
	Sec. 109. Construction and Preemption	**Sec. 108. Construction and Preemption**
	(f) Information Sharing Relationships	**(f) Information Sharing Relationships**
Stipulates that nothing in '(3)'	Stipulates that nothing in the title	Stipulates that nothing in the bill
- limits or modifies an existing information sharing relationship or prohibits or requires a new one,	- **(1)** limits or modifies an existing information sharing relationship or **(2)** prohibits or requires a new one.	[Similar to PCNA] or
——	——	requires use of the DHS sharing process under Sec. 105(c) [p. 26].
——	**Sec. 103(c)(3)** stipulates that nothing in (c)	**Sec. 104(c)(3)** stipulates that nothing in (c)
——	- authorizes information sharing other than as provided in (c),	[Identical to PCNA]
——	- permits unauthorized sharing of classified information, - authorizes federal surveillance of any person, - prohibits a federal entity, at the request of a nonfederal entity, from technical discussion of threat	——

NCPAA	PCNA	CISA
	indicators and defensive measures and assistance with vulnerabilities and threat mitigation, - prohibits otherwise lawful sharing by a nonfederal entity of indicators or defensive measures with DOD, or	
- limits otherwise lawful activity, or	[Similar to NCPAA]	[Identical to PCNA]
- impacts or modifies existing procedures for reporting criminal activity to appropriate law enforcement authorities, or participating in an investigation.	——	——
Requires the U/S-CIP to coordinate with stakeholders to develop and implement policies and procedures to coordinate disclosures of vulnerabilities as practicable and consistent with relevant international industry standards.	——	——
'(4) Network Awareness Authorization'	**(a) Authorization for Private-Sector Defensive Monitoring**	**(a) Authorization for Monitoring**
permits nonfederal, nongovernment entities, notwithstanding any other provision of law, to conduct network awareness, for cybersecurity purposes and to protect rights or property, of	**(1)** permits private entities, notwithstanding any other provision of law, to monitor, for cybersecurity purposes,	[Similar to PCNA]
- its own information systems,	[Similar to NCPAA]	[Identical to PCNA]
- with written consent, information systems of a nonfederal or federal entity, or	[Similar to NCPAA] or	[Similar to NCPAA] or
- the contents of such systems.	[Similar to NCPAA]	[Identical to PCNA]
Stipulates that nothing in '(4)' - authorizes network awareness other than as provided in the section, or	**(2)** Stipulates that nothing in (a) - authorizes monitoring other than as provided in the title,	[Identical to NCPAA]
- limits otherwise lawful activity,	[Similar to NCPAA]	[Similar to PCNA]
——	- authorizes federal surveillance of any person.	——
'(5) Defensive Measure Authorization'	**(b) Authorization for Operation of Defensive Measures**	**(b) Authorization for Operation of Defensive Measures**

NCPAA	PCNA	CISA
permits nonfederal, nongovernment entities to operate defensive measures, for cybersecurity purposes and to protect rights or property, that are applied to	**(1)** permits private entities to operate defensive measures, for a cybersecurity purpose and to protect rights or property, that are operated on	**(1)** permits private entities to operate defensive measures, for cybersecurity purposes and to protect rights or property, that are applied to
- its own information systems,	[Similar to NCPAA] or	[Similar to NCPAA]
- with written consent, information systems of a nonfederal or federal entity, or	- with written authorization, information systems of a nonfederal or federal entity, or	- with written consent, information systems of another [nonfederal] entity, or a federal entity with written consent of an authorized representative
- the contents of such systems,	——	——
notwithstanding any other provision of law, except that measures may not be used except as authorized in the section, and '(5)' does not limit otherwise lawful activity.	**(1)** notwithstanding any other provision of law, except **(3)** that measures may not be used except as authorized in (b), and (b) does not limit otherwise lawful activity.	**(1)** notwithstanding any other provision of law, except **(2)** [Identical to PCNA]
[No Corresponding Provision; however, the definition of defensive measure in Sec. 202(a) includes a similar restriction; see p. 17.]	**(2)** stipulates that (1) does not authorize operation of defensive measures that destroy, render wholly or partly unusable or inaccessible, or substantially harm an information system or its contents not owned by either the private entity operating the measure or a nonfederal or federal entity that provided written authorization to that private entity.	[No Corresponding Provision; however, the definition of defensive measure in Sec. 2 includes a similar restriction; see p. 17.]
——	**(e) No Right or Benefit** Stipulates that sharing of indicators with a nonfederal entity creates no right or benefit to similar information by any nonfederal entity.	**(f) No Right or Benefit** Stipulates that sharing of indicators with a [nonfederal] entity creates no right or benefit to similar information by any [nonfederal] entity.
'(6) Privacy and Civil Liberties Protections'	**Sec. 104(b) Privacy and Civil Liberties**	**Sec. 105(b) Privacy and Civil Liberties**
Requires the U/S-CIP,	**(1)** requires the AG,	**(1)** requires the AG,
in coordination with the DHS CPO and Chief Civil Rights and Civil Liberties Officer,	in consultation with appropriate federal agency heads and agency privacy and civil liberties officers,	in coordination with appropriate federal entity heads and in consultation with agency privacy and civil liberties officers,

NCPAA	PCNA	CISA
to establish and review annually policies and procedures on information shared with the NCCIC under the section.	to develop and review periodically guidelines on privacy and civil liberties to govern federal handling of cyber threat indicators obtained through the title's provisions.	to develop interim guidelines on privacy and civil liberties to govern federal handling of cyber threat indicators obtained through the bill's provisions;
[*Note:* No requirement for interim policies and procedures]	[*Note:* No distinction between requirements for interim and final versions of the guidelines]	**(2)** in coordination with appropriate federal entity heads and in consultation with agency privacy and civil liberties officers and relevant private entities with industry expertise, to promulgate, and review at least biennially, in coordination with appropriate agency heads and consultation with agency privacy and civil liberties officers and relevant private entities, final guidelines on privacy and civil liberties to govern federal handling of cyber threat indicators obtained through the bill's provisions
Requires that they apply only to DHS, consistent with the need for timely protection of information systems from and mitigation of cybersecurity risks and incidents, the policies and procedures	**(2)** requires that, consistent with the need for protection of information systems and threat mitigation, the guidelines	**(3)** [Similar to PCNA]
- be consistent with DHS FIPPs,	- be consistent with FIPPs in the White House National Strategy for Trusted Identities in Cyberspace [*Note:* The two versions of the principles are identical, except that the DHS version applies the principles to DHS whereas the White House document applies them to "organizations"],	**(a)(3)** requires that, consistent with the bill, applicable provisions of law and the FIPPs in the White House National Strategy for Trusted Identities in Cyberspace govern federal retention, use, and dissemination of information shared with the federal government under the bill;
- "reasonably limit, to the extent practicable, receipt, retention, use, and disclosure of cybersecurity threat indicators and defensive measures associated with specific persons" not needed for timely protection of systems and networks,	- limit receipt, retention, use, and dissemination of cybersecurity threat indicators containing personal information of or identifying specific persons,	**(b)(3)** - limit receipt, retention, use, and dissemination of cybersecurity threat indicators containing information that is personal or that identifies specific persons,
——	including by establishing processes for prompt destruction of information known not to be directly related to uses for cybersecurity purposes, setting limitations on retention of indicators, and notifying	including by establishing processes for timely destruction of information known not to be directly related to uses under the title, and setting limitations on retention of indicators, and requiring that

NCPAA	PCNA	CISA
	recipients that indicators may be used only for cybersecurity purposes, and,	recipients be informed that indicators may be used only for purposes authorized under the bill,
- minimize impacts on privacy and civil liberties,	- limit impacts on privacy and civil liberties of federal activities under the title, including	- limit impacts on privacy and civil liberties of federal activities under the bill,
- provide data integrity through prompt removal and destruction of obsolete or erroneous personal information unrelated to the information shared and retained by the NCCIC in accordance with this section,	guidelines for removal of personal and personally identifying information handled by federal entities under the title,	——
- include requirements to safeguard from unauthorized access or acquisition cyber threat indicators and defensive measures retained by the NCCIC,	- include requirements to safeguard from unauthorized access or acquisition cyber threat indicators	[Identical to PCNA]
identifying specific persons, including proprietary or business-sensitive information,	containing personal information of or identifying specific persons,	containing information that is personal or that identifies specific persons,
- protect the confidentiality of cyber threat indicators and defensive measures associated with specific persons, to the greatest extent practicable,	——	- protect the confidentiality of cyber threat indicators containing information that is personal or that identifies specific persons, to the greatest extent practicable,
- ensure that relevant constitutional, legal, and privacy protections are observed.	- be consistent with other applicable provisions of law,	[See (a)(3), p. 32, stating that applicable provisions of law will govern information sharing activities, consistent with the bill],
——	- include procedures to notify entities if a federal entity receiving information knows that it is not a cyber threat indicator,	[Similar to PCNA]
——	- include steps to ensure that dissemination of indicators is consistent with the protection of classified and other sensitive national security information.	[Similar to PCNA]
Stipulates that the U/S-CIP may consult with NIST in developing the policies and procedures.	——	——
Requires the DHS CPO and the Officer for Civil Rights and Civil Liberties, in consultation with the PCLOB, to submit to appropriate congressional committees	**(3)** requires the AG to submit to Congress	Requires the AG to submit to Congress

NCPAA	PCNA	CISA
the policies and procedures within 180 days of enactment and annually thereafter.	interim guidelines within 90 days of enactment and final guidelines within 180 days.	**(1)** interim guidelines within 60 days of enactment and **(2)** final guidelines within 180 days.
Requires the U/S-CIP, in consultation with the PCLOB and the DHS CPO and Chief Civil Rights and Civil Liberties Officer, to ensure public notice of and access to the policies and procedures.	——	**(1)** requires the AG to make the interim guidelines available to the public. [*Note:* There is no similar requirement for the final guidelines.]
Requires the DHS CPO to - monitor implementation of the policies and procedures, - submit to Congress an annual review on their effectiveness, - work with the U/S-CIP to carry out provisions in '(c)' on notification about violations of privacy and civil liberties policies and procedures and about information that is erroneous or in contravention of section requirements, - regularly review and update impact assessments as appropriate to ensure that all relevant protections are followed, and	——	——
- ensure appropriate sanctions for DHS personnel who knowingly and willfully conduct unauthorized activities under the section.	**(2)** requires that the AG's guidelines include appropriate sanctions for federal activities in contravention of them. [*Note:* The provision does not specify whether these sanctions are limited to violation of requirements for safeguarding information or the guidelines as a whole.]	**(b)(3)** [Identical to PCNA]
	Sec. 107. Oversight of Government Activities	**Sec. 107. Oversight of Government Activities**
	(b) Reports on Privacy and Civil Liberties.	**(b) Reports on Privacy and Civil Liberties.**
Requires the DHS IG, in consultation with the PCLOB and IGs of other agencies receiving shared indicators or defensive measures from the NCCIC, to submit a report to HSC and HSGAC within two years of enactment and periodically thereafter reviewing such information, including	**(2)** requires the IGs of DHS, the IC, DOJ, and DOD, in consultation with the IG Council, to jointly submit a report to Congress within two years of enactment and biennially thereafter, on	**(2)** requires the IGs of DHS, the IC, DOJ, DOD, and the Department of Energy, in consultation with the IG Council, to jointly submit a biennial report to Congress on

NCPAA	PCNA	CISA
- receipt, use, and dissemination of cybersecurity indicators and defensive measures shared with federal entities under the section,	- receipt, use, and dissemination of cybersecurity indicators and defensive measures shared with federal entities under the title,	[Similar to PCNA]
- information on NCCIC use of such information for purposes other than cybersecurity,	——	——
- types of information shared with the NCCIC,	- types of indicators shared with federal entities,	[Identical to PCNA]
- actions taken by NCCIC based on shared information;	- actions taken by federal entities as a result of receiving shared indicators,	[Identical to PCNA]
- metrics to determine impacts of sharing on privacy and civil liberties,	——	——
- a list of federal agencies receiving the information,	- a list of federal entities receiving the indicators,	[Identical to PCNA] and
- review of sharing of information within the federal government to identify inappropriate stovepiping of shared information, and	- review of sharing of indicators among federal entities to identify inappropriate barriers to sharing information,	[Identical to PCNA]
——	- procedures for sharing information and removal of personal and identifying information, and incidents involving improper treatment of it, and	——
- recommendations for improvements or modifications to sharing under the section.	- recommendations for improvements or modifications to authorities under the title.	**(3)** permits inclusion of recommendations for improvements or modifications to authorities under the bill.
——	Requires that the reports be submitted in unclassified form but permits a classified annex.	**(4)** [Similar to PCNA]
——	Requires public availability of unclassified parts of the reports.	——
——	**(1)** adds a new paragraph to Sec. 1061(e) of the Intelligence Reform and Terrorism Prevention Act of 2004:	——
Requires the DHS CPO and Chief Civil Rights and Civil Liberties Officer, in consultation with the PCLOB, the DHS IG, and senior privacy and civil liberties	**'(3)'** requires the PCLOB to	**(1)** [Similar to PCNA]

NCPAA	PCNA	CISA
officers of each federal agency receiving indicators or defensive measures shared with the NCCIC, to		
submit a biennial report to Congress	submit a biennial report to Congress and the President	[Similar to PCNA]
assessing impacts on privacy and civil liberties of federal activities under '(6)', including	assessing impacts of activities under the title on and sufficiency of policies, procedures, and guidelines in addressing concerns about privacy and civil liberties, including	assessing effects of the types of activities under on the bill on and sufficiency of policies, procedures, and guidelines in addressing concerns about privacy and civil liberties.
recommendations to minimize or mitigate such impacts.	recommendations for improvements or modifications to authorities under the title.	**(3)** permits inclusion of recommendations for improvements or modifications to authorities under the bill,
Requires that the two reports be submitted in unclassified form but permits a classified annex.	Requires that the reports be submitted in unclassified form but permits a classified annex.	**(4)** [Similar to PCNA]
——	Requires public availability of unclassified parts of the reports.	——
	(a) Biennial Report on Implementation	**(a) Biennial Report on Implementation**
——	**(1)** Adds to 'Sec. 111' of the National Security Act	——
	'(c) Biennial Report on Implementation'	
——	**'(1)'** requires the DNI to submit a report to Congress on implementation of the title, **(2)** within one year of enactment and **'(1)'** at least biennially thereafter, **'(2)'** including	**(1)** requires joint reports to Congress from - the heads of appropriate federal agencies and - the IGs of DHS, the IC, DOJ, DOD, and the Department of Energy, in consultation with the IG Council on implementation of the bill, within one year of enactment, covering the most recent one-year period, and at least biennially thereafter, covering the most recent two-year period, including
——	- review of types of indicators shared with the federal government, including	- review of types of indicators shared with the appropriate federal entities, including
——	——	the number of indicators received through the methods in Sec. 105(c),
——	——	the number of times shared information was used by a federal entity to prosecute an offense consistent with Sec. 105(d)(5),

NCPAA	PCNA	CISA
——	the degree to which such information may impact privacy and civil liberties of specific persons, along with quantitative and qualitative assessment of such impacts and adequacy of federal efforts to reduce them,	the degree to which such information may affect privacy and civil liberties of specific persons, along with quantitative and qualitative assessment of such effects and adequacy of federal efforts to reduce them, and including the number of notices issued with respect to failures to remove information that is personal or that identifies specific persons not directly related to a threat in accordance with Sec. 105(b)(3) procedures,
——	- assessment of sufficiency of policies, procedures, and guidelines to ensure effective and responsible sharing under Sec. 4 [sic] of PCNA,	- assessment of sufficiency of policies, procedures, and guidelines to ensure effective and responsible sharing under Sec. 105,
——	——	- effectiveness of real-time sharing under Sec. 105(c).
——	- sufficiency of procedures under Sec. 3 [sic] for timely sharing [*Note:* References 'Sec. 111(a)(1)' as added by the title; see p. 20],	- sufficiency of procedures under Sec. 103 for timely sharing,
——	- appropriateness of classification of indicators and accounting of security clearances authorized,	[Similar to PCNA]
——	- federal actions taken based on shared indicators, including appropriateness of subsequent use or dissemination under the title,	[Similar to PCNA]
——	- description of any significant federal violations of the requirements of the title, including assessments of all reports of federal personnel misusing information provided under the title and all disciplinary actions taken, and	- description of any significant federal violations of the requirements of the title,
——	- a summary of the number and types of nonfederal entities receiving classified indicators from the federal government and evaluation of risks and benefits of such sharing.	[Similar to PCNA]
——	- assessment of personal or personally identifying information not directly related to a threat that was shared by a nonfederal entity with the federal government in contravention to Sec. 3(d)(2) or within the government in contravention of Sec. 4(b)	——

NCPAA	PCNA	CISA
	guidelines. [*Note:* Intended reference to Sec. 103 and 104 respectively.]	
——	**'(3)'** permits reports to include recommendations for improvements or modifications to authorities and processes under the title.	[Similar to PCNA]
——	**'(4)'** requires that the reports be submitted in unclassified form but permits a classified annex.	[Similar to PCNA]
——	**'(5)'** requires public availability of unclassified parts of the reports.	——
'(7) Uses and Protection of Information'	**Sec. 103. Authorizations for Preventing, Detecting, Analyzing, and Mitigating Cybersecurity Threats**	**Sec. 104. Authorizations for Preventing, Detecting, Analyzing, and Mitigating Cybersecurity Threats**
	(d) Protection and Use of Information	**(d) Protection and Use of Information**
[Nonfederal Entities]		
Permits a nonfederal, nongovernment entity that shares indicators or defensive measures with the NCCIC to	**(3)** permits a nonfederal entity [*Note:* including government entities], for a cybersecurity purpose, to	**(3)** permits a [nonfederal] entity [*Note:* including government entities], for cybersecurity purposes, to
use, retain, or disclose indicators and defensive measures, solely for cybersecurity purposes.	use an "indicator or defensive measure shared or received under this section to monitor or operate a defensive measure on" its own information systems or those of other nonfederal or federal entities upon written authorization from them, with	use indicators or defensive measure shared or received under this section to monitor or operate a defensive measure that is applied to its own information systems or those of other entities upon written consent from them, with
Requires reasonable efforts prior to sharing to safeguard personally identifying information from unintended disclosure and unauthorized access or acquisition, and remove or exclude such information where it is reasonably believed when shared to be unrelated to a cybersecurity risk or incident.	[See (2), p. 29, describing requirements for removal of personal information.]	[See (2), p. 29, describing requirements for removal of personal information.]
Requires compliance with appropriate restrictions on subsequent disclosure or retention placed by a federal or nonfederal entity on indicators or defensive measures disclosed to other entities.	further use, retention, or sharing subject to lawful restrictions by the sharing entity or otherwise applicable provisions of law.	[Similar to PCNA]

NCPAA	PCNA	CISA
Stipulates that the information shall be deemed voluntarily shared.	——	——
Requires implementation and utilization of security controls to protect against unauthorized access or acquisition.	**(1)** requires implementation of appropriate security controls to protect against unauthorized access or acquisition. [*Note:* Also applies to nonfederal government entities.]	**(1)** Requires implementation and utilization of security controls to protect against unauthorized access or acquisition. [*Note:* Also applies to nonfederal government entities.]
Prohibits use of such information to gain an unfair competitive advantage.	——	**(3)** Prohibits use of such information other than as authorized in (d).
[Federal Entities]	**Sec. 104(d) Information Shared with or Provided to the Federal Government**	**Sec. 105(d) Information Shared with or Provided to the Federal Government**
Permits federal entities receiving indicators or defensive measures from the NCCIC or otherwise under the section to use, retain, or further disclose it solely for	**(5)** permits federal entities or personnel receiving indicators or defensive measures under the title to, consistent with otherwise applicable provisions of federal law, use, retain, or disclose it solely for	**(5)** [Similar to PCNA]
cybersecurity purposes.	a cybersecurity purpose,	[Identical to PCNA]
——	——	identifying a cybersecurity threat, - including a source or vulnerability, - use of an information system by a foreign adversary of terrorist,
[*Note:* Sec. 216 (see p. 55) permits use of information obtained from federal systems for investigating, prosecuting, disrupting, or otherwise responding to	"responding to, investigating, prosecuting, or otherwise preventing or mitigating"	"responding to or otherwise preventing or mitigating"
imminent threats of death or serious bodily harm	threats of death or serious bodily harm or offenses arising out of such threats,	imminent threats of death or serious bodily harm or
——	——	"serious economic harm, including a terrorist act or a use of a weapon of mass destruction,"
serious threats to minors, including sexual exploitation or threats to physical safety, and	"a serious threat to a minor, including sexual exploitation and threats to physical safety," and	[Identical to PCNA]
violations of 18 U.S.C. 1030 [computer fraud], or	- preventing, investigating, disrupting, or prosecuting offenses listed in 18 U.S.C. 1028-30, 3559(c)(2)(F), and Ch. 37 and 90 [computer fraud and identity theft,	[Similar to PCNA] or

NCPAA	PCNA	CISA
	espionage and censorship, protection of trade secrets, and serious violent felonies].	
——	——	
attempts or conspiracy to commit the above offenses.]	——	——
——	Prohibits federal disclosure, retention, or use for any purpose not permitted under (5).	[Similar to PCNA]
Requires reasonable efforts prior to sharing to safeguard personally identifying information from unintended disclosure and unauthorized access or acquisition, and remove or exclude such information where it is reasonably believed when shared to be unrelated to a cybersecurity risk or incident.	Stipulates that the policies, procedures, and guidelines in (a) [on provision of information to the federal government] and (b) [on privacy and civil liberties] of the title apply to such information.	Stipulates that the policies, procedures, and guidelines in (a) and (b) apply to such information, that confidentiality of information in indicators that is personal or that identifies specific persons must be protected and the information protected from unauthorized use or disclosure.
——	**'Sec. 111(a)(2)'** requires that procedures for sharing developed include methods for federal entities to assess, prior to sharing, whether an indicator contains information known to be personal or identifying of a specific person and to remove such information, or to implement a technical capability to remove <u>or exclude</u> such information.	**Sec. 103(b)(1)** requires that procedures for sharing developed include methods for federal entities to assess, prior to sharing, whether an indicator contains information known to be personal or that identifies a specific person and to remove such information, or to implement <u>and utilize</u> a technical capability to remove such information.
Requires implementation and utilization of security controls to protect against unauthorized access or acquisition.	**'Sec. 111(a)(2)'** requires that procedures for sharing developed by the DNI include requirements for federal entities to implement security controls to protect against unauthorized access to or acquisition of shared information.	Requires that procedures for sharing developed by the DNI include requirements for federal entities to implement <u>and utilize</u> security controls to protect against unauthorized access to or acquisition of shared information.
	Sec. 109(a) Prohibition of Surveillance	
Prohibits use in surveillance or collection activities to track an individual's personally identifiable information except as authorized in the section.	Stipulates that the title does not authorize DOD or any element of the IC to target a person for surveillance.	——
Stipulates that the indicators and defensive measures shared from a federal or nonfederal entity under the section shall be deemed to have been voluntarily shared.	**Sec. 104(d)(3)** stipulates that an indicator or defensive measure provided to the federal government under the bill shall be deemed voluntarily shared information.	**Sec. 105(d)(3)** stipulates that indicators and defensive measure provided to the federal government under the title shall be deemed voluntarily shared information.

NCPAA	PCNA	CISA
Stipulates that the information is exempt from disclosure under 5 U.S.C. 552 [the Freedom of Information Act (FOIA)] or nonfederal disclosure laws and withheld, without discretion, from the public under 5 U.S.C. 552(3)(B).	Stipulates that the information is exempt from disclosure under FOIA or nonfederal disclosure laws and withheld, without discretion, from the public under 5 U.S.C. 552(3)(B),	[Similar to PCNA]
——	except for information requiring disclosure in criminal prosecutions.	——
Prohibits federal use for regulatory purposes.	[*Note:* No specific corresponding prohibition, but Sec. 104(d)(5) above prohibits federal disclosure, retention, or use for any purpose other than those specified in the paragraph.]	**(5)** prohibits federal or nonfederal use to regulate lawful activities of an entity, including enforcement actions and activities relating to monitoring, defense, or sharing of indicators, except to inform development or implementation of authorized regulations relating to prevention or mitigation of threats to information systems and to procedures under the title.
Specifies that there is no waiver of applicable privilege or protection under law, including trade-secret protection;	**(1)** [Similar to NCPAA]	**(1)** [Similar to NCPAA]
Requires that the information be considered the commercial, financial, and proprietary information of the nonfederal entity when so designated by it.	**(2)** requires that, consistent with the title, the information be considered the commercial, financial, and proprietary information of the originating nonfederal source, when so designated by such source or nonfederal entity acting with written authorization from it.	**(2)** requires that, consistent with Sec. 104(c)(2), the information be considered the commercial, financial, and proprietary information of the [nonfederal] entity providing it, when so designated by the originating [nonfederal] entity or third party acting with written authorization from it.
Stipulates that the information is not subject to judicial doctrine or rules of federal entities on ex-parte communications.	**(4)** [Similar to NCPAA]	**(4)** [Similar to NCPAA]
[Nonfederal Government Entities]	[*Note:* See also Nonfederal Entities, p. 38.]	[*Note:* See also Nonfederal Entities, p. 38.]
Permits state, local, and tribal government to	**Sec. 103(d)(4)** permits state, local, and tribal government entities	**Sec. 104(d)(4)** permits state, local, and tribal government entities, with prior written consent of sharing entity or oral consent in exigent circumstances,
use, retain, or further disclose indicators or defensive measures shared under the section solely for.	to use shared cyber threat indicators for [*Note:* Purposes below are included by reference to specified provisions in Sec. 104(d)(5)]	to use shared cyber threat indicators for [*Note:* included by reference to specified provisions in Sec. 105(d)(5)]

NCPAA	PCNA	CISA
cybersecurity purposes.	a cybersecurity purpose,	
——	"responding to, investigating, prosecuting, or otherwise preventing or mitigating"	"responding to, or otherwise preventing or mitigating"
——	"a threat of death or serious bodily harm or an offense arising out of such a threat," or	"an imminent threat of death, serious bodily harm, or serious economic harm, including a terrorist act or a use of a weapon of mass destruction," or
——	"a serious threat to a minor, including sexual exploitation and threats to physical safety."	——
——	——	"preventing, investigating, disrupting, or prosecuting" offenses relating to fraud and identity theft, espionage and censorship, and protection of trade secrets. [*Note:* The bill cites provisions in title 18 of the U.S. Code.]
Requires reasonable efforts prior to sharing to safeguard personally identifying information from unintended disclosure and unauthorized access or acquisition, and remove or exclude such information where it is reasonably believed when shared to be unrelated to a cybersecurity risk or incident.	[See (2), p. 29, describing requirements for removal of personal information.]	[Similar to PCNA]
Stipulates that the information be considered "commercial, financial, and proprietary" if so designated by the provider.	[*Note:* Sec. 103(d)(3) stipulates that further use, retention, or sharing of information received by a nonfederal entity is subject to lawful restrictions by the sharing entity or otherwise applicable provisions of law. See Nonfederal Entities, p. 38.]	[Similar to PCNA]
Stipulates that the indicators and defensive measures shall be deemed voluntarily shared.	Stipulates that such shared indicators or defensive measures be deemed voluntarily shared and exempt from disclosure, and	Stipulates that such shared indicators be deemed voluntarily shared and exempt from disclosure, and
Requires implementation and utilization of security controls to protect against unauthorized access or acquisition.	**(1)** requires implementation of appropriate security controls to protect against unauthorized access or acquisition. [*Note:* Also applies to nonfederal nongovernment entities.]	**(1)** Requires implementation and utilization of security controls to protect against unauthorized access or acquisition. [*Note:* Also applies to nonfederal nongovernment entities.]
Exempts the information from disclosure under nonfederal disclosure laws or regulations.	Exempts the information from disclosure under nonfederal disclosure laws or regulations, except as required in criminal prosecutions.	**(4)** Exempts the information from disclosure under nonfederal disclosure laws or regulations.

NCPAA	PCNA	CISA
Prohibits use for regulation of lawful activities of nonfederal entities.	——	Prohibits use to regulate lawful activities of a [nonfederal] entity, including enforcement actions and activities relating to monitoring, defense, or sharing of indicators, except to inform development or implementation of authorized regulations relating to prevention or mitigation of threats to information systems.
'(8) Liability Exemptions'	**Sec. 106. Protection from Liability**	**Sec. 106. Protection from Liability**
	(a) Monitoring of Information Systems	**(a) Monitoring of Information Systems**
States that "no cause of action shall lie or be maintained in any court" against nonfederal, nongovernment entities for conducting network awareness under '(4)' in accordance with the section or	States that "no cause of action shall lie or be maintained in any court" against private entities for monitoring information systems under Sec. 103(a) conducted in accordance with the title or	[Similar to PCNA, but refers to Sec. 104(a)]
	(b) Sharing or Receipt of Cyber Threat Indicators	**(b) Sharing or Receipt of Cyber Threat Indicators**
for sharing indicators or defensive measures under '(3),' or a good-faith failure to act if sharing is done in accordance with the section.	for information sharing under Sec. 103(c) in accordance with the title or a good-faith failure to act if sharing is done in accordance with the title.	for information sharing under Sec. 104(c) in accordance with the title if sharing is done in accordance with the bill and, for sharing with the federal government after the earlier of submission of interim procedures under Sec. 105(a)(1) and guidelines under Sec. 105(b)(1) or 60 days after enactment, it uses the DHS process under Sec. 105(c)(1).
	(c) Willful Misconduct	**(c) Construction**
Stipulates that nothing in the section	**(1)** Stipulates that nothing in the section	Stipulates that nothing in the section
- requires dismissal of a cause of action against a nonfederal, nongovernment entity that engages in willful misconduct in the course of activities under the section.	requires dismissal of a cause of action against a nonfederal entity that engages in willful misconduct in the course of activities under the title, or	- requires dismissal of a cause of action against a [nonfederal] entity that engages in gross negligence or willful misconduct in the course of activities under the title, or
- undermines or limits availability of otherwise applicable common law or statutory defenses.	[Identical to NCPAA]	[Identical to NCPAA]

NCPAA	PCNA	CISA
Establishes the burden of proof as clear and convincing evidence from the plaintiff of injury-causing willful misconduct,	**(2)** [Similar to NCPAA]	——
Defines *willful misconduct* as an act or omission taken intentionally to achieve a wrongful purpose, knowingly without justification, and in disregard of risk of highly probable harm that outweighs any benefit.	**(3)** [Similar to NCPAA]	——
'(9) Federal Government Liability for Violations of Restrictions on the Use and Protection of Voluntarily Shared Information'	**Sec. 105. Federal Government Liability for Violations of Privacy or Civil Liberties**	
	(a) In General	
Makes the federal government liable to injured persons for intentional or willful violation of restrictions on federal disclosure and use under 'Sec. 226', with minimum damages of $1,000 plus	Makes the federal government liable to injured persons for intentional or willful violation of privacy and civil liberties guidelines under Sec. 104(b), with minimum damages of $1,000 plus	——
reasonable attorney fees as determined by the court and other reasonable litigation costs in any case under (a) where "the complainant has substantially prevailed."	[Identical to NCPAA]	——
	(b) Venue	
Stipulates the federal district courts where the case may be brought as the one in which the complainant resides or the principal place of business is located, the District of Columbia, or	[Identical to NCPAA]	——
where the federal department or agency that disclosed the information is located.	where the federal department or agency that violated the guidelines is located.	——
	(c) Statute of Limitations	
Sets the statute of limitations under '(i)' at two years from the date on which the cause of action arises.	Sets the statute of limitations under Sec. 105 at two years from the date on which the cause of action arises.	——

NCPAA	PCNA	CISA
	(d) Exclusive Cause of Action.	
Sets action under '(i)' as the exclusive remedy for violation of restrictions under '(i)(3),' '(i)(6),' or '(i)(7)(B)'.	Sets action under (d) as the exclusive remedy for federal violations under the title.	——
'(10) Anti-Trust Exemption'		**Sec. 104(e) Antitrust Exemption**
Exempts nonfederal entities from violation of antitrust laws for sharing indicators or defensive measures or providing assistance for cybersecurity purposes, provided that the action is taken to assist with preventing, investigating, or mitigating a cybersecurity risk or incident.	——	Exempts any two or more private entities from violation of antitrust laws, except as provided in Sec. 108(e) [p.46] for exchanging or providing indicators or assistance for cybersecurity purposes to help prevent, investigate, or mitigate a cybersecurity risk or incident.
'(11) Construction and Preemption'	**Sec. 109(b) Otherwise Lawful Disclosures**	**Sec. 108(a) Otherwise Lawful Disclosures**
Nothing in the section may be construed to	Nothing in the title or the amendments made by it shall be construed to	Nothing in the title shall be construed to
- limit or prohibit otherwise lawful disclosures or participation in an investigation by a nonfederal entity of information to any other federal or nonfederal entity,	- limit or prohibit otherwise lawful disclosures by a nonfederal entity of information to any other federal or nonfederal entity, or	- limit or prohibit otherwise lawful disclosures by a [nonfederal] entity of information to any federal or other entity, or
——	any otherwise lawful use by a federal entity, whether or not the disclosures duplicate those made under the title,	any otherwise lawful use by a federal entity, even when the disclosures duplicate those made under the title,
	(c) Whistle Blower Protections	**(b) Whistle Blower Protections**
- prohibit or limit disclosures protected under 5 U.S.C. 2302(b)(8), 5 U.S.C. 7211, 10 U.S.C. 1034, 50 U.S.C. 3234, or similar provisions of federal or state law,	- prohibit or limit disclosures protected under 5 U.S.C. 2302(b)(8), 5 U.S.C. 7211, 10 U.S.C. 1034, or similar provisions of federal or state law,	- prohibit or limit disclosures protected under 5 U.S.C. 2302(b)(8), 5 U.S.C. 7211, 10 U.S.C. 1034, 50 U.S.C. 3234, or similar provisions of federal or state law,
	(d) Protection of Sources and Methods	**(c) Protection of Sources and Methods**
——	- affect federal enforcement actions on classified information or conduct of authorized law-enforcement or intelligence activities, or modify the authority of the President or federal entities to protect and control dissemination of classified information, intelligence sources and methods, and U.S. national security,	- affect federal enforcement actions on classified information or conduct of authorized law-enforcement or intelligence activities, or modify the authority of federal entities to protect classified information, sources and methods, and U.S. national security,

NCPAA	PCNA	CISA
	(e) Relationship to Other Laws	
- affect any requirements under other provisions of law for nonfederal entities providing information to federal entities,	[Similar to NCPAA]	[Similar to NCPAA]
	(g) Preservation of Contractual Obligations and Rights	**(g) Preservation of Contractual Obligations and Rights**
- change contractual relationships between nonfederal entities or them and federal entities or abrogate trade-secret or intellectual property rights,	[Similar to NCPAA]	[Similar to NCPAA]
	(h) Anti-Tasking Restriction	**(h) Anti-Tasking Restriction**
- permit the federal government to require nonfederal entities to provide it with information, or to condition	- permit the federal government to require nonfederal entities to provide it with information, or to condition	- permit a federal entity to require nonfederal entities to provide it or another entity with information, or to condition
sharing of indicators or defensive measures on provision by such entities of indicators or defensive measures, or	sharing of indicators on provision of indicators, or	sharing of indicators on provision of indicators to a federal or other entity, or
award of grants, contracts, or purchases on such provision,	award of grants, contracts, or purchases on such provision,	award of grants, contracts, or purchases on such provision,
	(i) No Liability for Non-Participation	**(i) No Liability for Non-Participation**
- create liabilities for any nonfederal entities that choose not to engage in the voluntary activities authorized in the section,	- create liabilities for any nonfederal entities that choose not to engage in a voluntary activity authorized in the title, or	- create liabilities for any nonfederal entities that choose not to engage in the voluntary activities authorized in the title,
	(j) Use and Retention of Information	**(j) Use and Retention of Information**
- authorize or modify existing federal authority to retain and use information shared under the title for uses other than those permitted under the section,	- authorize or modify existing federal authority to retain and use information shared under the title for uses other than those permitted under the title.	- authorize or modify existing federal authority to retain and use information shared under the title for uses other than those permitted under the title,
- restrict or condition sharing for cybersecurity purposes among nonfederal entities or require sharing by them with the NCCIC, or	——	——
		(e) Prohibited Conduct

NCPAA	PCNA	CISA
- "permit price-fixing, allocating a market between competitors, monopolizing or attempting to monopolize a market, or exchanges of price or cost information, customer lists, or information regarding future competitive planning."	——	- "permit price-fixing, allocating a market between competitors, monopolizing or attempting to monopolize a market, boycotting, or exchanges of price or cost information, customer lists, or information regarding future competitive planning," or
		(m) Authority of Secretary of Defense to Respond to Cyber Attacks
——	——	- "limit the authority of the Secretary of Defense to develop, prepare, coordinate, or, when authorized by the President to do so, conduct a military cyber operation in response to a malicious cyber activity carried out against the United States or a United States person by a foreign government or an organization sponsored by a foreign government or a terrorist organization."
	(k) Federal Preemption	**(k) Federal Preemption**
Specifies that the section supersedes state and local laws relating to its provisions	**(1)** Specifies that the title supersedes state and local laws relating to its provisions.	**(1)** Specifies that the title supersedes state and local laws relating to its provisions.
——	**(2)** Stipulates that the title does not supersede state and local laws on use of authorized law enforcement practices and procedures.	[Similar to PCNA]
——	**(3)** Stipulates that, except with respect to exemption from disclosure under Sec. 103(b)(4), the title does not supersede state and local law on private entities performing utility services except to the extent that they restrict activities under the title.	——
Requires the Secretary to develop policies and procedures for direct reporting by the NCCIC Director of significant risks and incidents.	——	——
Requires the Secretary to build on existing mechanisms to promote public awareness about the importance of securing information systems.	——	——

NCPAA	PCNA	CISA
Requires a report from the Secretary within 180 days of enactment to HSC and HSGAC on efforts to bolster collaboration on cybersecurity with international partners.	——	——
Requires the Secretary, within 60 days of enactment, to publicly disseminate information about ways of sharing information with the NCCIC, including enhanced outreach to CI owners and operators.	——	——
Sec. 204. Information Sharing and Analysis Organizations		
Amends Sec. 212 of the HSA to	——	——
(1) broaden the functions of ISAOs to include cybersecurity risk and incident information beyond that relating to critical infrastructure, and	——	——
(2) add by reference the definitions of *cybersecurity risk* and *incident* in 6 U.S.C. 148(a).	——	——
Sec. 207. Security and Resiliency of Public Safety Communications; Cybersecurity Awareness Campaign		**Sec. 404. Enhancement of Emergency Services**
(a) In General		
Adds two new sections to the HSA:	——	——
		(a) Collection of Data
		Requires the Secretary, acting through the NCCIC and in coordination with appropriate federal entities and the Director for Emergency Communications, to establish, within 90 days of enactment, a process for reporting of data by a Statewide Interoperability Coordinator on cybersecurity risks or incidents involving systems or networks used by state emergency response providers as defined in 6 U.S.C. 101.

NCPAA	PCNA	CISA
'Sec. 230. Security and Resiliency of Public Safety Communications'		**(b) Analysis of Data**
Requires the NCCIC to coordinate with the DHS Office of Emergency Communications to assess information on cybersecurity incidents involving public safety communications to facilitate continuous improvement in those communications.	——	Requires the Secretary, acting through the NCCIC and in coordination with appropriate entities and the Director for Emergency Communications and in consultation with the NIST Director, to conduct, within one year of enactment, integration and analysis of the data reported in (a) to develop information and recommendations on security and resilience measures for systems and networks used by state emergency response providers.
		(c) Best Practices
——	——	**(1)** requires the NIST Director to use the results under (b) and other relevant information to facilitate and support development of methods to reduce cybersecurity risks to emergency response providers using the process described in 15 U.S.C. 272(e) [relating to public/private collaboration in reducing such risks].
——	——	**(2)** requires a publicly available report to Congress on those methods from the NIST Director.
'Sec. 231. Cybersecurity Awareness Campaign'		
'(a) In General'		
Requires the U/S-CIP to develop and implement an awareness campaign on risks and best practices for mitigation and response, including at a minimum public service announcements and information on best practices that are vendor- and technology-neutral.	——	——
'(b) Consultation'		
Requires consultation with a wide range of stakeholders.	——	——
'Sec. 232. National Cybersecurity Preparedness Consortium'		

NCPAA	PCNA	CISA
'(a) In General'		
Authorizes the Secretary to establish the National Cybersecurity Preparedness Consortium to	——	——
'(b) Functions'		
- provide cybersecurity training to state and local first responders and officials, - establish a training curriculum for them using the DHS Community Cyber Security Maturity Model, - provide technical assistance for improving capabilities, - conduct training and simulation exercises, - coordinate with the NCCIC to help states and communities develop information sharing programs, and - coordinate with the National Domestic Preparedness Consortium to incorporate cybersecurity into emergency management functions.	——	——
'(c) Members'		
Stipulates that members be academic, nonprofit, and government partners with prior experience conducting cybersecurity training and exercises in support of homeland security.	——	——
(b) Clerical Amendment		
Amends the table of contents of the act to include the new sections.	——	——
——	**Sec. 108. Report on Cybersecurity Threats** **(a) Report Required** Requires the DNI, in consultation with heads of other appropriate elements of the IC, to submit within 180 days of enactment a report to the House and Senate Intelligence Committees on cybersecurity threats to the U.S. national security and economy, including attacks, theft, and data breaches.	**Sec. 109. Report on Cybersecurity Threats** **(a) Report Required** Requires the DNI, in coordination with heads of other appropriate elements of the IC, to submit within 180 days of enactment a report to the House and Senate Intelligence Committees on cybersecurity threats, including attacks, theft, and data breaches.

NCPAA	PCNA	CISA
	(b) Contents	**(b) Contents**
——	Requires that the report include	Requires that the report include
——	**(1)** assessments of current U.S. intelligence sharing and cooperation relationships with other countries on such threats directed against the United States and threatening U.S. national security interests, the economy, and intellectual property, identifying the utility of relationships, participation by elements of the IC, and possible improvements,	**(1)** assessments of current U.S. intelligence sharing and cooperation relationships with other countries on such threats directed against the United States and threatening U.S. national security interests, the economy, and intellectual property, specifically identifying the utility of relationships, participation by elements of the IC, and possible improvements,
——	**(2)** a list and assessment of countries and nonstate actors constituting the primary sources of such threats,	**(2)** [Similar to PCNA]
——	**(3)** description of how much U.S. capabilities to respond to or prevent such threats to the U.S. private sector are degraded by delays in notification of the threats,	**(3)** [Similar to PCNA]
——	**(4)** assessment of additional technologies or capabilities that would enhance the U.S. ability to prevent and respond to such threats, and	**(4)** [Similar to PCNA]
——	**(5)** assessment of private-sector technologies or practices that could be rapidly fielded to assist the IC in preventing and responding to such threats.	**(5)** [Identical to PCNA]
	(c) Form of Report	**(d) Form of Report**
——	Requires that the report be unclassified but permits a classified annex.	Requires that the report be made available in unclassified and classified forms.
	(d) Public Availability of Report	
——	Requires that the unclassified portion of the report be publicly available.	——
		(c) Additional Report
——	——	Requires that the DNI submit a report to the House Foreign Affairs and Senate Foreign Relations

NCPAA	PCNA	CISA
		Committees with the information in (b)(2) at the time the report required in (a) is submitted.
	(e) Intelligence Community Defined	**(e) Intelligence Community Defined**
——	Defines intelligence community as in 50 U.S.C. 3003.	[Identical to PCNA]
Sec. 210. Assessment		
Requires the Comptroller General, within two years of enactment, to submit a report to HSC and HSGAC assessing implementation of the title and, as practicable, findings on increased sharing at NCCIC and throughout the United States.	——	——
Sec. 213. Prohibition on New Regulatory Authority	**Sec. 109(l) Regulatory Authority**	**Sec. 108(l) Regulatory Authority**
Stipulates that the title does not grant DHS new authority to promulgate regulations or set standards relating to cybersecurity for nonfederal, nongovernmental entities.	Stipulates that the title does not authorize **(1)** promulgation of regulations or **(2)** establishment of regulatory authority not specified by the title, or **(3)** duplicative or conflicting regulatory actions.	Stipulates that the title does not authorize **(1)** promulgation of regulations or **(2)** establishment <u>or limitation of</u> regulatory authority not specified by the bill, or **(3)** duplicative or conflicting regulatory actions.
Sec. 214 Sunset		
Ends all requirements for reports in the title seven years after enactment.	——	——
Sec. 215. Prohibition on New Funding		
Stipulates that the title does not authorize additional funds for implementation and must be carried out using available amounts.	——	——
Sec. 216. Protection of Federal Information Systems		**Title II—Federal Cybersecurity Enhancement**
		Sec. 201. Short Title
——	——	Federal Cybersecurity Enhancement Act of 2015
		Sec. 202. Definitions
——	——	Defines, in the title,

NCPAA	PCNA	CISA
——	——	*Agency:* As in 44 U.S.C. 3502.
——	——	*Agency information system:* As in Sec. 228 of the HSA as added by Sec. 203(a).
——	——	*Appropriate Congressional Committees:* The Senate Homeland Security and Governmental Affairs Committee and the House Committee on Homeland Security.
——	——	*Cybersecurity Risk:* As in 6 U.S.C. 148(a).
——	——	*Director: The OMB Director.*
——	——	*Information System:* As in 44 U.S.C. 3502.
——	——	*Intelligence Community:* As in 50 U.S.C. 3003.
——	——	*National Security System:* As in 40 U.S.C. 11103.
——	——	*Secretary:* The Secretary of Homeland Security.
——	——	**Sec. 203. Improved Federal Network Security**
(a) In General		**(a) In General**
Adds a new section to the HSA.	——	Amends the HSA by **(1)** renumbering Sec. 228 [on clearances] as Sec. 229, **(4)** adding a new Sec. 228, **(2)** renumbering Sec. 227 [on cyber incident response plans] as Sec. 228(c), **(3)** renumbering "second section 226" [on the NCCIC, see p. 19] as Sec. 227, **(5)** amending the reference to Sec. 226 in Sec. 228(c) to read "Sec. 227," and **(6)** adding a new Sec. 230.
		'Sec. 228. Cybersecurity plans'
		'(a) Definitions'
——	——	Defines, in the section,

NCPAA	PCNA	CISA
——	——	*Agency Information System:* "An information system used or operated by an agency or by another entity on behalf of an agency."
——	——	*Cybersecurity Risk, Information System, Intelligence Community,* and *National Security System:* As in Sec. 202:
		'(b) Intrusion Assessment Plan'
——	——	**'(1)'** requires the Secretary to develop and implement, in coordination with the OMB Director, a plan to identify and remove intruders from agency information systems.
——	——	**'(2)'** stipulates that the plan does not apply to DOD, NSS, or the IC.
'Sec. 233. Available Protection of Federal Information Systems'		**'Sec. 230. Federal Intrusion Detection and Prevention System'**
		'(a) Definitions'
——	——	Defines, in the section,
——	——	*Agency Information:* "Information collected or maintained by or on behalf of an agency."
——	——	*Agency, Agency Information System, Cybersecurity Risk,* and *Information System:* As in Sec. 202.
		'(b) Requirement'
'(a) In General'		**'(1) In General'**
Requires the Secretary to deploy and operate, to make available to agencies with or without reimbursement, capabilities,	——	**'(1)'** Requires the Secretary to deploy, operate, and maintain, to make available to agencies with or without reimbursement, capabilities,
including technologies for continuous diagnostics, detection, prevention, and mitigation, for protecting federal information systems and their contents from cybersecurity risks.		- to detect cybersecurity risks in network traffic to and from agency systems, and - to stop such traffic or remove the risks.

NCPAA	PCNA	CISA
——	——	**'(2)'** Requires the Secretary to regularly modify technologies and employ new ones to improve capabilities.
'(b) Activities'		**'(c) Activities'**
Authorizes the Secretary to	——	Authorizes the Secretary to
'(1)' access information traveling to or from <u>or stored on</u> an agency system regardless of location, and permits agency heads to disclose such information to the Secretary or a private entity assisting the Secretary, notwithstanding any other provision of law that would otherwise restrict such disclosure,	——	**'(1)'** access information traveling to or from an agency system regardless of location, and permits agency heads to disclose such information to the Secretary or a private entity assisting the Secretary, notwithstanding any other provision of law that would otherwise restrict such disclosure,
'(2)' obtain assistance through agreements or otherwise from private entities for implementing technologies under '(a),'	——	**'(2)'** [Similar to NCPAA]
'(3)' use, retain, and disclose information obtained under this section only to protect federal systems and their contents,	——	**'(3)'** [Similar to NCPAA]
or with approval of the AG, to respond to violations of 18 U.S.C. 1030 [on computer fraud and related activities], threats of death or serious bodily harm, serious threats to minors, including sexual exploitation and threats to physical safety, or attempts or conspiracy to commit such offenses.	[*Note:* Sec. 104(d)(5) has related provisions for information shared with the federal government (see p. 39).]	[*Note:* Sec. 105(d)(5) has related provisions for information shared with the federal government (see p. 3939).]
——	——	Requires the Secretary to
——	——	**'(4)'** regularly test, and utilize when appropriate, commercial and noncommercial technologies to improve capabilities,
——	——	**'(5)'** establish a pilot for acquiring, testing, and deploying such technologies,
——	——	**'(6)'** periodically update privacy impact assessments required under 44 U.S.C. 3501 note, and

NCPAA	PCNA	CISA
——	——	**'(7)'** ensure that - activities under the section are reasonably necessary to protect systems and their information, - information accessed by the Secretary is retained no longer than reasonably necessary for such protection, - notice is provided to users about access to communications for purposes of such protection, and - operation of the intrusion detection and prevention capabilities is implemented pursuant to governing policies and procedures.
		'(d) Private Entities'
'(c) Conditions'		**'(1) Conditions'**
Requires that the agreements under '(b)(2)' bar	——	Prohibits a private entity described in (2) from
- disclosure of identifying information reasonably believed to be unrelated to a cybersecurity risk except to DHS or the disclosing agency, and	——	- disclosure of network traffic from an agency system without consent from the disclosing agency, and
- use of information accessed under the section by a private entity for any purpose other than protecting agency information systems and their contents or administration of the agreement.	——	- use of network traffic accessed under the section by a private entity for any purpose other than protecting agency information systems and their contents or administration of the agreement under '(c)(2)' or as part of another contract with the Secretary.
'(d) Limitation'		**'(2) Limitation on Liability'**
States that no cause of action shall lie against a private entity for assistance provided in accordance with this section and an agreement under '(b)(2).'	——	States that no cause of action shall lie against a private entity for assistance provided in accordance with this section and an agreement pursuant to '(b)(2).'
		'(3) Rule of Construction'
——	——	Stipulates that '(2)' does not authorize an Internet service provider to break a user agreement without the customer's consent.
		'(e) Attorney General Review'

NCPAA	PCNA	CISA
——	——	Requires the AG to review policies and procedures for the program under this section to ensure consistency with applicable communications law.
		(b) Prioritizing Advanced Security Tools
——	——	Requires the OMB Director and the Secretary, in consultation with appropriate agencies, to **(1)** review and update and **(2)** brief HSGAC and HSC on government-wide policies and programs to ensure appropriate prioritization and use of monitoring tools within agency networks.
		(c) Agency Responsibilities
——	——	**(1)** Requires the head of each federal agency to begin using the capabilities under 'Sec. 230(b)(1)' between agency systems an any other systems by the later of one year after enactment or two months after the Secretary makes the capabilities available, **(2)** except for DOD, NSS, and the IC.
——	——	**(3)** defines, for (c) only, *Agency Information System* to mean "an information system owned or operated by an agency." [*Note:* this definition excludes systems operated on behalf of an agency; see p. 54.]
——	——	**(4)** stipulates that (c) does not limit agencies from applying capabilities under 'Sec. 230(b)(1)' at the discretion of agency heads or as provided in relevant policies, directives, and guidelines.
(b) Clerical Amendment		**(d) Table of Contents Amendment**
Amends the table of contents of the HSA to include the new section.	——	Amends the table of contents of the HSA to include the changes made by this section.
		Sec. 207. Termination
		(a) In General
——	——	Terminates authorities provided under 'Sec. 230' seven years after enactment.

NCPAA	PCNA	CISA
		(b) Rule of Construction
——	——	Stipulates that (a) does not affect limitations on liability for private entities under 'Sec. 230(d)(2)' for assistance rendered before the termination date in (a) or as otherwise authorized.
		Title IV. Other Cyber Matters
Sec. 217. Sunset	**Sec. 112. Sunset**	**Sec. 409. Effective Period**
		(a) In General
Terminates the provisions in the title seven years after enactment.	[Identical to NCPAA]	Terminates the provisions in the bill ten years after enactment, except that
		(b) Exception
——	——	actions shall continue in effect if authorized and occurring under the bill or information obtained pursuant to it before the termination date.
Sec. 220. GAO Report on Impact Privacy and Civil Liberties	**Sec. 111. Comptroller General Report on Removal of Personal Identifying Information**	
	(a) Report	
Requires a GAO report to HSC and HSGAC within five years of enactment assessing the impacts of NCCIC activities on privacy and civil liberties.	Requires a GAO report to Congress within three years of enactment on federal actions to remove personal information from threat indicators pursuant to Sec. 104(b).	——
	(b) Form	
——	Requires that the report be unclassified but permits a classified annex.	——
		Sec. 110. Conforming Amendment
——	——	Amends Sec. 941(c)(3) of the FY2013 National Defense Authorization Act (10 U.S.C. 2224 note) to permit sharing by the Secretary of Defense of threat indicators and defensive measures consistent with the

NCPAA	PCNA	CISA
		procedures promulgated by the AG and the Secretary under Sec. 105 of the bill.

Source: CRS.

Notes: See "Notes on the Table."

Table 2. Summaries of Sections in NCPAA and CISA: Federal Cybersecurity

Sections with No Corresponding Provisions in Other Bills

Cybersecurity of Federal Agencies and Information Systems

NCPAA: Sec. 205. Streamlining of Department of Homeland Security Cybersecurity and Infrastructure Protection Organization

(a) Cybersecurity and Infrastructure Protection Directorate

Renames the DHS National Protection and Programs Directorate as the Cybersecurity and Infrastructure Protection. [*Sic.*]

(b) Senior Leadership of the Cybersecurity and Infrastructure Protection Directorate

Provides a specific title for the undersecretary in charge of critical infrastructure protection as U/S-CIP. Also adds two deputy undersecretaries, one for cybersecurity and the other for infrastructure protection. Does not require new appointments for current officeholders and specifies that appointment of the undersecretaries does not require Senate confirmation.

(c) Report

Requires a report to HSC and HSGAC from the U/S-CIP within 90 days of enactment on the feasibility of becoming an operational component of DHS. If that is determined to be the best option for mission fulfillment, requires submission of a legislative proposal and implementation plan. Also requires that the report include plans for more effective execution of the cybersecurity mission, including expediting of information sharing agreements.

NCPAA: Sec. 209. Report on Reducing Cybersecurity Risks in DHS Data Centers

Requires a report to HSC and HSGAC within one year of enactment on the feasibility of creating an environment within DHS for reduction in cybersecurity risks in data centers, including but not limited to increased compartmentalization of systems with a mix of security controls among compartments.

CISA: Sec. 204. Advanced Internal Defenses

(a) Advanced Network Security Tools

(1) requires the Secretary to include advanced—including commercial, free, and open-source—tools in the Continuous Diagnostics and Mitigation Program.

(2) requires the OMB Director to develop and implement a plan to ensure that agencies use advanced network tools to detect and mitigate intrusions and anomalous activity.

(b) Improved Metrics

Requires the Secretary to collaborate with the OMB Director to review and update metrics used to measure security under 44 U.S.C. 3554 [FISMA] to include "measures of intrusion and incident detection and response times."

(c) Transparency and Accountability

Requires the Director, in consultation with the Secretary to increase public transparency on agency cybersecurity posture, including displaying metrics on federal websites for as many agencies and department components as practicable.

(d) Maintenance of Technologies

Revises 44 U.S.C. 3553(b)(6)(B) [FISMA] to require the Secretary to operate and maintain, as well as deploy, continuous diagnostics and mitigation tools to agencies upon request.

(e) Exception

Stipulates that the section requirements do not apply to DOD, NSS, or the IC.

Cybersecurity of Federal Agencies and Information Systems

CISA: Sec. 205. Federal Cybersecurity Requirements

(a) Implementation of Federal Cybersecurity Standards

Requires the Secretary, in consultation with the OMB Director, to issue binding operational directives, consistent with 44 U.S.C. 3553, to assist the Director in ensuring timely agency adoption of and compliance with standards and policies promulgated under 40 U.S.C. 11331.

(b) Cybersecurity Requirements at Agencies

(1) requires the head of each agency, within one year of enactment and consistent with FISMA and 40 U.S.C. 11331, to
- identify sensitive and mission-critical agency data consistent with the inventories required under 44 U.S.C. 3505,
- assess access controls to such data as well as the need for readily accessible storage and for individuals to access the data,
- render such data indecipherable to unauthorized users,
- implement a single sign-on trusted identity platform, developed by the Administrator of General Services in collaboration with the Secretary, for individuals accessing agency public websites that require user authentication, and
- implement identity management consistent with 15 U.S.C. 7464, including multi-factor authentication, for remote access to and each user account with elevated privileges on an agency system, except

(2) systems for which the agency head has personally certified to the OMB Director that
- operational requirements related to the system and articulated in the certification would make implementation excessively burdensome,
- the requirements are unnecessary for securing the system and its contents,
- the agency has taken all steps needed to secure the system and its contents, and
- the agency head or designee has submitted the certification to HSGAC and HSC and the agency authorizing committees.

(3) stipulates that the section does not
- alter the authority of the Secretary or the Directors of OMB or NIST in implementing FISMA, or
- affect NIST processes or requirements for coordination of the development of standards and guidelines in 44 U.S.C. 3553(a)(4), or discourage continuous improvement and advances in technology, standards, policies, and guidelines promoting federal information security. technology, standards, policies, and guidelines used to promote Federal information security.

(c) Exception

Stipulates that the section requirements do not apply to DOD, NSS, or the IC.

CISA: Sec. 206. Assessment; Reports

(a) Definitions

Defines, in the section,

Intrusion Assessment Plan: The plan required under 'Sec. 228(b)(1)' of HSA [see p. 54].

Intrusion Assessments: Actions taken under the plan to identify and remove intruders in agency systems.

Intrusion Detection and Prevention Capabilities: Those required in 'Sec. 230(b)' of the HSA [see p. 54].

(b) Third Party Assessment

Requires a GAO study within three years of enactment on the effectiveness of efforts to secure agency systems, including the intrusion plan and capabilities for detection and prevention.

(c) Reports to Congress

(1) Requires the Secretary, within six months of enactment and annually thereafter, to submit reports to HSGAC and HSC on implementation of intrusion detection and prevention capabilities, including
- descriptions of privacy controls and

Cybersecurity of Federal Agencies and Information Systems

- technologies, including commercial and noncommercial, and capabilities used to detect risks in network traffic and to prevent traffic associated with risks from moving to or from agency systems,

-for each iteration of the capabilities, types and numbers of identifiers and techniques used to detect risks in network traffic,

- instances where the capabilities detected risks and blocked associated traffic,

- description of the pilot required under Sec. 230(c)(5) [see p. 55], including the numbers of new technologies tested and participating agencies.

Requires the OMB Director, within 18 months of enactment, to include, in the annual FISMA report to Congress (44 U.S.C. 3553(c)), analysis of agency application of the capabilities, with

- the degree to which each agency has applied the capabilities to its systems,

- a list by agency of the number of instances where the capabilities detected a risk in network traffic, the indicators, identifiers, and techniques used for detection, and the number of instances where such traffic was blocked.

(2) requires the OMB Director to submit the intrusion assessment plan to HSGAC and HSC within six months of enactment and with 30 days of each subsequent update, and

within one year of enactment, to include in the annual FISMA report to Congress

- a description of implementation of the plan,

- findings of assessments conducted pursuant to it,

- advanced tools in the Continuous Diagnostics and Mitigation Program in Sec., 204(a)(1),

- results of the Secretary's assessment of best federal cybersecurity practices pursuant to Sec. 205(a) [*Note:* That provision refers to standards and policies but not best practices], and

- a list by agency of compliance with Sec. 205(b) requirements.

Requires the Director, within one year of enactment, to submit to HSGAC and HSC a copy of the plan required by Sec. 204(a)(2) and the metrics required by Sec. 204(b).

Sec. 207(a) [see p. 57] terminates the reporting requirements under Sec. 206(c) seven years after enactment.

CISA: Sec. 208. Identification of Information Systems Relating to National Security

(a) In General

Requires, within 180 days of enactment, **(1)** the DNI and the OMB Director, in coordination with other agency heads, to

- identify unclassified systems that may give an adversary the ability to derive information that would be considered classified,

- assess the risks from breaches of those systems and the costs and mission impacts to agencies from designating such systems as NSS, and

- to report those findings to HSGAC, HSC, and the House and Senate Intelligence Committees.

(b) Form

Requires that the report be unclassified but permits a classified annex.

(c) Exception

Stipulates that the section requirements do not apply to DOD, NSS, or the IC.

(d) Rule of Construction

Stipulates that the section does not designate any system as NSS.

Cybersecurity of Federal Agencies and Information Systems

CISA: Sec. 209. Direction to Agencies

(a) In General

Adds a new subsection to 44 U.S.C. 3553 [FISMA]:

'(h) Direction to Agencies'

'(1)' Except for systems described in 44 U.S.C. 3553(d) or (e) [NSS and mission-critical systems of DOD and the IC], permits the Secretary, in response to a substantial known or reasonably suspected threat to agency information security, to issue an emergency directive to the agency head to take lawful actions to protect the system or mitigate the threat.

'(2)' Requires the Secretary to

- establish, in coordination with the OMB Director, procedures on when such a directive may be issued, including criteria, privacy and civil liberties protections, and notice to potentially affected third parties,

- specify the reasons for and duration of the directive,

- minimize impacts by adopting the least intrusive security measures possible for the shortest practicable period,

- notify the OMB Director and the heads of affected agencies immediately upon issuance of a directive,

- consult with the NIST Director about directives implementing NIST standards and guidelines,

- consider applicable standards and guidelines under 40 U.S.C. 11331 and ensure that directives do not conflict with them, and

- submit annually to the appropriate congressional committees a report on the specific actions taken under '(h)(1).'

'(3)' permits the Secretary, notwithstanding 44 U.S.C. 3554 [on federal agency responsibilities under FISMA], to authorize, without delegation, the capabilities under 'Sec. 230(b)(1)' [see p. 54] to ensure the security of agency systems, consistent with applicable law, if the Secretary

- determines that there is an imminent threat to them, an emergency directive is not likely to result in a timely response, and the risk outweighs adverse consequences of action,

- provides notice prior to action to the OMB Director and the head and CIO of affected agencies, and within seven days to the appropriate congressional committees and the authorizing committees for the agencies, including the actions taken, and the reasons for and duration of them, and

- authorizes the use of the capabilities in accordance with advance procedures developed in coordination with the OMB Director and in consultation with federal agency heads and submitted to Congress.

'(4)' limits the actions of the Secretary to "protect[ing] agency information from unauthorized access, use, disclosure, disruption, modification, or destruction" or requiring remediation of or protection against risks to agency information or parts of systems used or operated by an agency or by another organization on its behalf.

'(i) Annual Report to Congress'

Requires an annual report by the OMB Director to the appropriate congressional committees on actions taken under 44 U.S.C. 3553(a)(5) [on overseeing agency compliance with FISMA requirements] and

'(j)' Appropriate Congressional Committees Defined

Defines, in this section, *Appropriate Congressional Committees* to mean the House and Senate Committees on Appropriations, HSGAC, HSC, the House Committees on Oversight and Government Reform and on Science, Space, and Technology.

(b) Conforming Amendment

Modifies 44 U.S.C. 3554(a(1)(B) [requiring agencies to comply with FISMA requirements] to include the emergency directives under this section.

Cybersecurity of Federal Agencies and Information Systems

CISA: Title III. Federal Cybersecurity Workforce Assessment

CISA: Sec. 301. Short Title

Federal Cybersecurity Workforce Assessment Act of 2015

CISA: Sec. 302. Definitions

Defines, in this title,

Appropriate Congressional Committees: The House and Senate Committees on Armed Services and on Intelligence, HSGAC, HSC, the House Committee on Oversight and Government Reform, and the Senate Committee on Commerce, Science, and Transportation.

Director: The Director of the Office of Personnel Management.

Roles: As in the National Initiative for Cybersecurity Education's Cybersecurity Workforce Framework.

CISA: Sec. 303. National Cybersecurity Workforce Measurement Initiative

(a) In General

Requires each agency head to **(1)** identify all positions in the agency requiring cybersecurity performance or other "cyber-related" functions, and **(2)** assign the corresponding employment code in accordance with (b). [*Note:* "Cyber" is not defined in the bill but generally refers broadly to matters associated with information and communications technology.]

(b) Employment Codes

(1) requires the Secretary of Commerce, acting through NIST, to update the NICE Cybersecurity Workforce Framework to include a corresponding coding structure, within 180 days of enactment.

Requires the establishment of procedures to implement the NICE coding structure to identify all federal positions with cyber-related functions,
- by the OPM Director, in coordination with the NIST Director and the DNI, within nine months of enactment for civilian positions,
- by the Secretary of Defense, within 18 months of enactment for noncivilian positions.

Requires the head of each agency within three months after development of those procedures, to

submit a report to appropriate congressional committees of jurisdiction that identifies
- the percentage of personnel with cyber-related functions currently holding appropriate industry-recognized certifications as identified in the NICE framework,
- the level of preparedness of other cyber personnel to take certification exams, and
- a strategy for mitigating gaps with appropriate training and certification.

establish procedures for
- identifying all encumbered and vacant positions with cyber-related functions as defined by the NICE coding structure, and
- assigning appropriate employment codes to each position, using agreed standards and definitions.

(2) requires agency heads to assign codes to each cyber-related position within one year of establishment of those procedures.

(c) Progress Report

Requires the OPM Director to submit a report on implementation of the section to the appropriate congressional committees within 180 days of enactment.

Cybersecurity of Federal Agencies and Information Systems

CISA: Sec. 304. Identification of Cyber-Related Roles of Critical Need

(a) In General

Requires agency heads, beginning within one year after their assignment of employment codes and in consultation with the OPM and NIST Directors and the Secretary of Homeland Security, to identify annually critically needed cyber-related workforce roles and to submit to the OPM Director a report describing and substantiating those needs.

(b) Guidance

Requires the OPM Director to provide agencies timely guidance for identifying those roles of critical need, including cyber-related roles with acute and emerging skill shortages.

(c) Cybersecurity Needs Report

Requires the OPM Director, within two years of enactment and in consultation with the Secretary, to identify critical cyber-related workforce needs across all agencies and submit a report on implementation of the section to the appropriate congressional committees.

Sec. 305. Government Accountability Office Status Reports

Requires GAO to analyze and monitor implementation of Secs. 303 and 304, and submit a report describing the status of implementation within three years of enactment.

CISA: Sec. 401. Study on Mobile Device Security

(a) In General

Requires the Secretary, within one year of enactment and in consultation with the NIST Director, to **(1)** complete a study on security threats to federal mobile devices and **(2)** submit an unclassified report to Congress, with a classified annex if necessary on findings, along with recommendations, deficiencies, and the plan described in (b).

(b) Matters Studied

Requires the Secretary, in carrying out the study under (a)(1), to

(1) assess the evolution of mobile security techniques from a desktop approach and whether they are adequate to meet current challenges,

(2) assess the effect that threats to federal mobile devices may have on the cybersecurity of federal systems and networks, except for NSS, DOD, and the IC,

(3) develop recommendations, based on industry standards and best practices, to address the threats,

(4) identify deficiencies in current authorities that might inhibit the ability of the Secretary to address the security of federal mobile devices, except for NSS, DOD, and the IC, and

(5) develop a plan for accelerated adoption of secure mobile technology by DHS.

(c) Intelligence Community Defined

Defines intelligence community as in 50 U.S.C. 3003.

CISA: SEC. 406. Federal Computer Security

(a) Definitions

Defines, in this section,

Covered System: As in 40 U.S.C. 11103 or a federal system providing access to personally identifiable information.

Covered Agency: An agency operating a covered system.

Logical Access Control: "A process of granting or denying specific requests to obtain and use information and related information processing services."

Cybersecurity of Federal Agencies and Information Systems
Multi-Factor Logical Access Controls: Two of more of - information known to a user, - an access device provided to a user, and - a unique biometric characteristic of a user. *Privileged User:* "A user who, by virtue of function or seniority, has been allocated powers within a covered system, which are significantly greater than those available to a majority of users." **(b) Inspector General Reports on Covered Systems** **(1)** requires the IG of each covered agency to submit, within 240 days of enactment, a report to the appropriate congressional committees of jurisdiction, including information described in (2). **(2)** requires that the report include, for covered systems in the agency, descriptions of - the logical access standards used by the agency, including an aggregate list and whether the agency is using multi-factor controls, - the logical access controls for privileged users, - for agencies not using such controls, the reasons they are not being used, - data security management practices, including policies and procedures used to conduct software inventories and associated licenses, capabilities used to monitor and detect threats, including data loss prevention and digital rights management, how the agency is using those capabilities, and reasons why not for agencies not using them, and - policies and procedures to ensure that entities providing services are implementing the data management practices. **(3)** permits the reports to be based on other reports, audits, or evaluations, and to be submitted as parts of other reports. **(4)** requires that the reports be unclassified but permits a classified annex.

Source: CRS.

Notes: See "Notes on the Table."

Table 3. Summaries of Sections in NCPAA and CISA: Critical Infrastructure Cybersecurity

Sections with No Corresponding Provisions in Other Bills

Critical Infrastructure Cybersecurity

NCPAA: Sec. 206. Cyber Incident Response Plans

(a) In General

Amends Sec. 227 of the HSA to change "Plan" to "Plans" in the title, to specify the U/S-CIP as the responsible official, and to add a new subsection:

'(b) Updates to the Cyber Incident Annex to the National Response Framework'

Requires the Secretary, in coordination with other agency heads and in accordance with the National Cybersecurity Incident Response Plan, to update, maintain, and exercise regularly the Cyber Incident Annex to the DHS National Response Framework.

(b) Clerical Amendment

Amends the table of contents of the act to reflect the title change made by (a).

NCPAA: Sec. 208. Critical Infrastructure Protection Research and Development

(a) Strategic Plan; Public-Private Consortiums

Adds a new section to the HSA:

'Sec. 318. Research and Development Strategy for Critical Infrastructure Protection'

'(a) In General'

Requires the Secretary to submit to Congress within 180 days of enactment, and biennially thereafter, a strategic plan to guide federal R&D in technology relating to both cyber- and physical security for CI.

'(b) Contents of Plan'

Requires the plan to include
- CI risks and technology gaps identified in consultation with stakeholders and a resulting risk and gap analysis,
- prioritized needs based on that analysis, emphasizing technologies to address rapidly evolving threats and technology and including clearly defined roadmaps,
- facilities and capabilities required to meet those needs,
- current and planned programmatic initiatives to foster technology advancement and deployment, including collaborative opportunities, and
- progress on meeting plan requirements.

'(c) Coordination'

Requires coordination between the DHS Under Secretaries for Science and Technology and for the National Protection and Programs Directorate. [*Note:* Sec. 205 renames the latter position as the U/S-CIP.]

'(d) Consultation'

Requires the Under Secretary for Science and Technology to consult with CI Sector Coordinating Councils, heads of other relevant federal agencies, and state, local, and tribal governments as appropriate.

(b) Clerical Amendment

Amends the table of contents of the act to include the new section.

NCPAA: Sec. 211. Consultation

Requires a report from the U/S-CIP on the feasibility of a prioritization plan in the event of simultaneous multi-CI incidents.

Critical Infrastructure Cybersecurity

NCPAA: Sec. 212. Technical Assistance

Requires the DHS IG to review US-CERT and ICS-CERT operations to assess their capacity for responding to current and potentially increasing requests for technical assistance from nonfederal entities.

NPAA: Sec. 218. Report on Cybersecurity Vulnerabilities of United States Ports

Requires a report with recommendations from the Secretary to HSC, HSGAC, House Committee on Transportation and Infrastructure, and Senate Committee on Commerce, Science, and Transportation within 180 days of enactment on cybersecurity vulnerabilities for the ten ports that the Secretary determines are at greatest risk of an incident.

NPAA: Sec. 219. Report on Cybersecurity and Critical Infrastructure

Authorizes the Secretary to consult with sector-specific entities on a report to HSC and HSGAC on federally funded cybersecurity R&D with private-sector efforts to protect privacy and civil liberties while protecting CI, including promoting R&D for secure and resilient design and construction, enhanced modeling of impacts from incidents or threats, and facilitating incentivization of investments to strengthen cybersecurity and resilience of CI.

CISA: SEC. 405. Improving Cybersecurity in the Health Care Industry

(a) Definitions

Defines, in the section,

Business Associate, Covered Entity Health Care Clearinghouse; Health Care Provider; and *Health Plan:* As in 45 C.F.R. 160.103.

Health Care Industry Stakeholder: Any of the following—a health plan, health care clearinghouse, health care provider, patient advocate, pharmacist, developer of health information technology, laboratory, pharmaceutical or medical device manufacturer, or other stakeholder as determined necessary by the HHS Secretary for purposes of (d)(1), (d)(3), or (e).

Secretary: The HHS Secretary.

(b) Report

Requires the HHS Secretary, within one year of enactment, to submit to the Senate Committee on Health, Education, Labor, and Pensions and the House Committee on Energy and Commerce a report on the preparedness of the health care industry for responding to cybersecurity threats.

(c) Contents of Report

Requires that the report include, with respect to the internal response of the HHS Department to emerging cybersecurity threats,

(1) identification of the HHS official responsible for leading and coordinating departmental efforts regarding industry threats, and

(2) a plan for each relevant departmental division and subdivision on how they will address such threats, including communication among with other divisions and subdivisions on efforts to address the threats and division of responsibilities among personnel.

Critical Infrastructure Cybersecurity

(d) Health Care Industry Cybersecurity Task Force

(1) requires the HHS Secretary, within 60 days of enactment and in consultation with the NIST Director and the Secretary of Homeland Security, to convene health care industry stakeholders, cybersecurity experts, and appropriate federal entities as determined by the HHS Secretary to establish a task force to
- analyze how other industries have implemented cybersecurity strategies and safeguards,
- analyze challenges and barriers faced by private entities (but not including state, tribal, or local governments) in the health care industry in securing against cyberattacks,
- review challenges faced by covered entities and business associates in securing networked medical devices and other software and systems connecting to electronic health records,
- provide the HHS Secretary with information to disseminate to stakeholders for improving their preparedness and responses to cybersecurity threats affecting the health care industry, which **(3)** the Secretary must disseminate with 60 days after termination of the task force,
- **(1)** establish a plan to create a single federal system for sharing information on actionable intelligence regarding such threats in near real time, with no fee to recipients, and including which entity may be best suited to serve as the central conduit for such sharing, and
- report to Congress on the findings and recommendations of the task force.

(2) terminates the task force one year after enactment.

(4) Stipulates that (d) does not limit the antitrust exemptions under Sec. 104(e) or liability protections under Sec. 106.

(e) Cybersecurity Framework

(1) requires the HHS Secretary to establish, through a collaborative process with the Secretary of Homeland Security, health care industry stakeholders, NIST, and other federal entities the HHS Secretary determines appropriate, a single, national, health-specific cybersecurity framework that
- establishes a common set of voluntary, consensus-based, and industry-led standards and other measures for cost-effectively reducing cybersecurity risks to health care organizations,
- supports voluntary adoption and implementation efforts,
- is consistent with security and privacy regulations under relevant provisions of the Health Insurance Portability and Accountability Act and the Health Information Technology for Economic and Clinical Health Act, and
- is updated regularly and applicable to a range of health care organizations.

(2) Stipulates that (e) does not grant the HHS Secretary authority to audit health care organizations for compliance with the voluntary framework or to mandate, direct, or condition awarding of federal grants, contracts, or purchases on such compliance.

(3) stipulates that nothing in the title subjects health care organizations to liability for choosing not to engage in the voluntary activities under (e).

CISA: Sec. 407. Strategy to Protect Critical Infrastructure at Greatest Risk

(a) Definitions

Defines, in this section,

Appropriate Agency: The applicable sector-specific agency or the federal entity that regulates a covered entity.

Appropriate Agency Head: the head of an appropriate agency.

Covered Entity: An entity identified pursuant to Sec. 9(a) of Executive Order 13636, on identifying CI where a cybersecurity incident could result in catastrophic effects.

Appropriate Congressional Committees: The House and Senate Intelligence Committees, HSGAC, HSC, The Senate Committees on Energy and Natural Resources and on Commerce, Science, and Transportation, and the House Energy and Commerce Committee.

Secretary: the Secretary of Homeland Security

Critical Infrastructure Cybersecurity
(b) Status of Existing Cyber Incident Reporting
(1) requires the Secretary, within 120 days of enactment and in conjunction with the appropriate agency head, to submit to the appropriate congressional committees the extent to which each covered entity reports to DHS or the appropriate agency head in a timely manner significant intrusions of information systems essential to the operation of CI.
(2) permits the report to include a classified annex.
(c) Mitigation Strategy Required for Critical Infrastructure at Greatest Risk
(1) requires the Secretary, within 180 days of enactment and in conjunction with the appropriate agency head, to conduct an assessment and develop a strategy addressing each covered entity to ensure that, to the greatest extent feasible, a cybersecurity incident affecting the entity would not reasonably result in catastrophic effects.
(2) requires the strategy to include - an assessment of whether each entity should be required to report incidents, - a description of security gaps identified that must be addressed, and - additional statutory authority needed to reduce the likelihood of an incident with catastrophic effects.
(3) requires the Secretary to submit the assessment and strategy to the appropriate congressional committees.
(4) permits the assessment and strategy to include classified annexes.

Source: CRS.

Notes: See "Notes on the Table."

Table 4. Summaries of Sections in NCPAA and CISA: Other Cybersecurity Provisions

Sections with No Corresponding Provisions in Other Bills

Other Cybersecurity Provisions

CISA: SEC. 402. Department of State International Cyberspace Policy Strategy

(a) In General

Requires the Secretary of State to produce a comprehensive strategy on U.S. international cyberspace policy within 90 days of enactment.

(b) Elements

Requires that the strategy include

(1) a review of the actions and activities of the secretary of state supporting the goal of the president's 2011 International Strategy for Cyberspace,

(2) an action plan to guide diplomacy by the Secretary of State, including activities with foreign countries to develop norms for behavior, and review of existing discussions in multilateral for a to obtain agreements on such norms,

(3) a review of alternative concepts on norms offered by prominent countries, including China, Russia, Brazil, and India,

(4) a detailed description of threats to U.S. national security in cyberspace, including infrastructure, intellectual property, and privacy, from countries and state-sponsored and private actors,

(5) a review of policy tools available to the President to deter such actors, including those in Executive Order 13694, and

(6) a review of the Office of the Coordinator for Cyber Issues and other resources required by the Secretary of State to conduct norm-building activities.

(c) Consultation

Requires the Secretary of State, in preparing the strategy, to consult with other federal agencies, the private sector, and U.S. nongovernmental organizations with recognized foreign policy, national security, and cybersecurity credentials and expertise.

(d) Form of Strategy

Requires that the strategy be unclassified but permits a classified annex.

(e) Availability of Information

Requires the Secretary of State to **(1)** make the strategy publicly available and **(2)** brief the Senate Foreign Relations and House Foreign Affairs Committees on it, including any material in a classified annex.

CISA: Sec. 403. Apprehension and Prosecution of International Cyber Criminals

(a) International Cyber Criminal Defined

Defines, in this section,

International Cyber Criminal: An individual **(1)** who is believed to have committed a cybercrime or intellectual property crime against U.S. interests or citizens, or **(2)** for whom a U.S. arrest warrant has been issued or an international wanted notice has been circulated by Interpol.

(b) Consultations for Noncooperation

Requires the Secretary of State or designee to consult with appropriate government officials of countries in which international cyber criminals are physically present and from which extradition is not likely, to determine what actions those governments have taken to apprehend and prosecute the criminals and to prevent them from criminal activities against U.S. interests or citizens.

Other Cybersecurity Provisions
(c) Annual Report **(1)** requires the Secretary of State to submit an annual report to **(3)** the House and Senate Appropriations, Intelligence, and Judiciary Committees, the House Foreign Affairs and Senate Foreign Relations Committees, HSC, HSGAC, the House Banking, Housing, and Urban Affairs Committee, and the Senate Financial Services Committee, including **(1)** - the number of international cyber criminals located in other countries, by country, and noting from which ones extradition is not likely, - the nature and number of significant discussions by State Department officials with officials of other countries, including the names of those countries, on ways to thwart or prosecute such criminals, and - the names, crimes charged, country of extradition, and country of previous residence for each such criminal extradited to the United States in the previous year, and **(2)** requires that the report be unclassified to the maximum extent possible but permits a classified annex.
CISA: Sec. 408. Stopping the Fraudulent Sale of Financial Information of People of the United States Amends 18 U.S.C. 1029(h) by broadening the entities for which an offense against them is covered to include any organized under laws of the United States, states, the District of Columbia, or U.S. territories, and by deleting the requirement that the offense involve articles used to assist in committing it that are within or pass through U.S. jurisdiction.

Source: CRS.

Notes: See "Notes on the Table."

Author Information

Eric A. Fischer
Senior Specialist in Science and Technology

Acknowledgments

This report was originally coauthored by Stephanie M. Logan while serving as a CRS intern and research assistant from January to August 2015. Her insights and other contributions were invaluable.

Disclaimer

This document was prepared by the Congressional Research Service (CRS). CRS serves as nonpartisan shared staff to congressional committees and Members of Congress. It operates solely at the behest of and under the direction of Congress. Information in a CRS Report should not be relied upon for purposes other than public understanding of information that has been provided by CRS to Members of Congress in connection with CRS's institutional role. CRS Reports, as a work of the United States Government, are not subject to copyright protection in the United States. Any CRS Report may be reproduced and distributed in its entirety without permission from CRS. However, as a CRS Report may include copyrighted images or material from a third party, you may need to obtain the permission of the copyright holder if you wish to copy or otherwise use copyrighted material.