



**Congressional
Research Service**

Informing the legislative debate since 1914

Cybersecurity and Information Sharing: Comparison of House and Senate Bills in the 114th Congress

Eric A. Fischer

Senior Specialist in Science and Technology

Stephanie M. Logan

Research Assistant

August 5, 2015

Congressional Research Service

7-5700

www.crs.gov

R44069

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 have been submitted, a managers amendment has been circulated, and a cloture motion was filed on August 3. Presumably, if the Senate passes CISA or another bill on information sharing, any inconsistencies between that bill 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. 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. In general, however, CISA and PCNA are more similar to each other than either is to NCPAA, although a number of those differences are provisions with no corresponding language in the other bills and potentially could be included in any final legislation.

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 114 th Congress.....	4
Overview of the Legislative Proposals.....	4
Selected Issues.....	6
Side-by-Side Comparison of NCPAA, PCNA, and CISA.....	12
Managers Amendment to CISA.....	12
Glossary of Abbreviations in the Table.....	13
Notes on the Table.....	14

Tables

Table 1. Side-by-Side Comparison of the Two Titles of H.R. 1560 as Passed by the House—PCNA (Title I) and NCPAA (Title II)—and S. 754 (CISA).....	15
---	----

Contacts

Author Contact Information.....	56
---------------------------------	----

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 reported 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.

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 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 R42409, *Cybersecurity: Selected Legal Issues*, by Edward C. Liu et al.; 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 have been filed. The analysis in this report is based on the reported version of the bill. Changes that would be made by a widely circulated substitute are discussed in the section on "Managers Amendment to CISA."

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 proposal¹⁴ (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

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.

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.

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 DHS Secretary, 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

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>).

sharing, and includes some provisions to facilitate sharing of classified cybersecurity information with appropriate entities.

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 CTTIC in PCNA. The Obama Administration had not posted a statement of Administration policy on CISA as of August 4. However, the Department of Homeland Security has raised concerns about some of its provisions,²⁷ although a White House spokesman has reportedly stated that the Administration supports passage of the bill.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

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.

²⁸ Cory Bennett, “White House Endorses Senate Cyber Bill,” *The Hill*, August 4, 2015, <http://thehill.com/policy/cybersecurity/250241-white-house-endorses-senate-cyber-bill>.

need to reduce such barriers best be balanced against any risks to well-established protections?

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

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://src.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-intel-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>.

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 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

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>.

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 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

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.

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 (continued...)

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 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

(...continued)

Eric A. Fischer et al.

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.”

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 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,

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.

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 a side-by-side comparison of provisions in NCPAA and PCNA as passed by the House and CISA as reported to the Senate.

Managers Amendment to CISA

A widely circulated managers' amendment to CISA would make some changes that are not reflected in the table but are summarized here:

- Narrows the definition of *defensive measure* in Sec. 2(7) to expressly exclude measures that provide unauthorized access to information systems.
- Expands the definition of *private entity* in Sec. 2(15) to include utilities other than electric utilities.
- Narrows the authorized uses of shared information by nonfederal entities in Sec. 4(c)(1) to cybersecurity purposes (certain law-enforcement uses would still be permitted for nonfederal governments with prior consent under Sec. 4(d)(4)).
- Makes the Secretary of Homeland Security responsible along with the Attorney General for developing policies and procedures for federal receipt of shared cyber threat indicators and defensive measures under Sec. 5(a).
- Clarifies that communications about previously shared indicators between a federal and private entity through the DHS process in Sec. 5(c) are for the purpose of describing threats or developing defensive measures.
- Deletes the provision in Sec. 5(d)(5) permitting use of shared information for law enforcement purposes relating to serious violent felonies under 18 U.S.C. §3559(c)(2)(F), which cover crimes that are arguably not related to cybersecurity.
- Eliminates the express exemption under the Freedom of Information Act (FOIA) for cybersecurity information under Sec. 10.
- Makes other clarifying or technical changes, for example, changing “personal information of or identifying a specific person” to “personal information or information that identifies a specific person” at several places in the bill, and requiring that the Director of National Intelligence submit a separate report to the House Foreign Affairs and Senate Foreign Relations Committees when submitting the report required under Sec. 9.

Glossary of Abbreviations in the Table

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
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
ODNI	Office of the Director of National Intelligence
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
U.S.	United States
U.S.C.	United States Code
US-CERT	United States Computer Emergency Readiness Team
U/S-CIP	DHS Under Secretary for Cybersecurity and Infrastructure Protection

Notes on the Table

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

- Related provisions in the two titles are adjacent to each other, with NCPAA serving as the basis for comparison.⁵³ As a result, many provisions of PCNA appear out of sequence in the 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 as a visual aid to highlight differences with a corresponding provision in the other bill 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 table—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.
- In cases where a provision of PCNA 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. 28, a provision from Sec. 103 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, 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 corresponding provision.

See the “Glossary of Abbreviations in the Table” for meanings of abbreviations used therein.

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

Table I. Side-by-Side Comparison of the Two Titles of H.R. 1560 as Passed by the House—PCNA (Title I) and NCPAA (Title II)—and S. 754 (CISA)

NCPAA	PCNA	CISA
<p>“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.”</p>	<p>“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.]</p>	<p>[Identical to PCNA]</p>
<p>Sec. 201. Short Title</p>	<p>Sec. 101. Short Title</p>	<p>Sec. 1. Short title; table of contents</p>
<p>National Cybersecurity Protection Advancement Act of 2015</p>	<p>Protecting Cyber Networks Act</p>	<p>Cybersecurity Information Sharing Act of 2015</p>
<p>Sec. 202. National Cybersecurity and Communications Integration Center</p>	<p>_____</p>	<p>_____</p>
<p>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.]</p>	<p>_____</p>	<p>_____</p>
<p>(a) In General</p>	<p>Sec. 110. Definitions</p>	<p>Sec. 2. Definitions</p>
<p>Amends existing definitions in 6 U.S.C. 148(a):</p>	<p>_____</p>	<p>_____</p>
<p><i>Cybersecurity Risk:</i> Excludes actions solely involving violations of consumer terms of service or licensing agreements from the definition.</p>	<p>_____</p>	<p>_____</p>
<p><i>Incident:</i> 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.”</p>	<p>_____</p>	<p>_____</p>
<p>Adds the following definitions:</p>	<p>Agency: As in 44 U.S.C. 3502.</p>	<p>[Identical to PCNA]</p>

NCPAA	PCNA	CISA
—	—	<i>Antitrust Laws:</i> 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.
—	<i>Appropriate Federal Entities:</i> Departments of Commerce, Defense, Energy, Homeland Security, Justice, and the Treasury; and Office of the ODNI.	[Identical to PCNA]
—	<i>Cybersecurity Threat:</i> An action unprotected by the 1 st 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]
<i>Cyber Threat Indicator:</i> <u>Technical</u> information necessary to describe or identify	<i>Cyber Threat Indicator:</i> Information <u>or a physical object</u> necessary to describe or identify	<i>Cyber Threat Indicator:</i> 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 <u>reasonably</u> appear to have “the purpose of gathering technical information related to a cybersecurity <u>risk</u> ,”	<u>anomalous patterns of</u> communications that appear to have “the purpose of gathering technical information related to a cybersecurity <u>threat or security vulnerability</u> ,”	[Identical to PCNA]
- a method for defeating a security control or <u>technical control</u> ,	- a method of defeating a security control or <u>exploiting a security vulnerability</u> ,	[Identical to PCNA]
- “a <u>technical</u> vulnerability including anomalous <u>technical behavior</u> that may become a vulnerability,”	- a <u>security</u> vulnerability or anomalous activity indicating the existence of one,	[Identical to PCNA]
- a method of causing a legitimate user of an information system or its contents to “ <u>inadvertently</u> enable the defeat of a <u>technical or</u>	- a method of causing a legitimate user of an information system or its contents to <u>unwittingly</u> enable defeat of a <u>security control or</u>	[Identical to PCNA]

NCPAA	PCNA	CISA
<p><u>operational</u> control,”</p> <p>- 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</p> <p>- actual or potential harm from an incident, including exfiltration of information; or</p> <p>- any other cybersecurity <u>risk</u> attribute that cannot be used to identify specific persons believed to be unrelated to the risk, and</p> <p>disclosure of which is not prohibited by law.</p> <p>- any combination of the above.</p> <p><i>Cybersecurity Purpose:</i> Protecting an information system or its contents from a cybersecurity <u>risk or incident</u> or identifying a <u>risk or incident</u> source.</p> <p><i>Defensive Measure:</i> An “action, device, procedure, <u>signature</u>, technique, or other measure <u>applied to</u> an information system” or its contents that “<u>detects</u>, prevents or mitigates a known or suspected cybersecurity <u>risk or incident</u>” or <u>attributes that could help defeat security controls</u>, but not including “a measure that destroys, renders unusable, or substantially harms an information system” or its contents not operated by that <u>nonfederal</u> entity, <u>except a state, local, or tribal government</u>, or by another <u>nonfederal</u> or federal entity that consented to such actions.</p> <p>—</p> <p>[Note: No corresponding provision, but <i>Information</i></p>	<p><u>exploitation of a security vulnerability.</u></p> <p>- “malicious cyber command and control,” [Note: Definition of this term below includes remote identification, access, or use of an information system or its contents.]</p> <p>[Identical to NCPAA]</p> <p>- any other cybersecurity <u>threat</u> attribute the disclosure of which is not prohibited by law.</p> <p>—</p> <p><i>Cybersecurity Purpose:</i> Protecting (including by using defensive measures) an information system or its contents from a cybersecurity <u>threat or security vulnerability</u> or identifying a <u>threat</u> source.</p> <p><i>Defensive Measure:</i> An “action, device, procedure, technique, or other measure” <u>executed on</u> an information system or its contents that “prevents or mitigates a known or suspected cybersecurity <u>threat or security vulnerability</u>.”</p> <p>[No Corresponding Provision; however, the authority to operate defensive measures in Sec. 103(b) includes a similar restriction; see p. 30];</p> <p><i>Federal Entity:</i> A U.S. department or agency, or any component thereof.</p> <p><i>Information System:</i> As in 44 U.S.C. 3502.</p>	<p>[Identical to PCNA]</p> <p>[Identical to NCPAA]</p> <p>[Identical to PCNA]</p> <p>[Identical to PCNA]</p> <p>- “any combination thereof.”</p> <p><i>Cybersecurity Purpose:</i> Protecting an information system or its contents from a cybersecurity <u>threat or security vulnerability</u>.</p> <p><i>Defensive Measure:</i> An “action, device, procedure, <u>signature</u>, technique, or other measure” <u>applied to</u> an information system that “<u>detects</u>, prevents or mitigates a known or suspected cybersecurity <u>threat or security vulnerability</u>.”</p> <p>but not including “a measure that destroys, renders unusable, or substantially harms an information system” or its contents not operated by that <u>private</u> entity, or by another <u>entity</u> or federal entity that consented to such actions.</p> <p>[Identical to PCNA]</p> <p>[Identical to PCNA]</p>

NCPAA	PCNA	CISA
System is already defined in 6 U.S.C. 148 as 44 U.S.C. 3502.]		
—	<i>Local Government:</i> A political subdivision of a state.	[Identical to PCNA]
[Note: No corresponding provision, but the definition of <i>Cyber Threat Indicator</i> 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.]	<i>Malicious Cyber Command and Control:</i> “A method for unauthorized remote identification of, access to, or use of an information system” or its contents.	[Identical to PCNA]
—	<i>Malicious Reconnaissance:</i> A method, associated with a known or suspected cybersecurity threat, for probing or monitoring an information system to discern its vulnerabilities.	[Identical to PCNA]
<u>Network Awareness:</u> Scanning, identifying, acquiring, monitoring, logging, or <u>analyzing</u> the contents of an information system.	<u>Monitor:</u> Scanning, identifying, <u>acquiring, or otherwise possessing</u> 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]	<i>Non-Federal Entity:</i> A private entity or nonfederal government or agency thereof (<u>including personnel</u>), but not including foreign powers as defined in 50 U.S.C. 1801.	<i>Entity:</i> A private entity or nonfederal government or agency thereof, but not including foreign powers as defined in 50 U.S.C. 1801.
<i>Private Entity:</i> A nonfederal entity that is an <u>individual</u> , nonfederal government utility or “an entity performing utility services,” or private group, organization, proprietorship, partnership, trust, cooperative, corporation, or other commercial or nonprofit entity,	<i>Private Entity:</i> A <u>person</u> , nonfederal government utility, or	<i>Private Entity:</i> A <u>person</u> , nonfederal government <u>electric</u> utility, or
including personnel.	[Identical to NCPAA]	[Identical to NCPAA]
—	including personnel, but not including a foreign power as defined in 50 U.S.C. 1801.	[Identical to PCNA]
—	<i>Real Time:</i> Automated, machine-to-machine system processing of cyber threat indicators where the	—

NCPAA	PCNA	CISA
<p><i>Security Control:</i> The management, operational, and technical controls used to protect an information system and <u>the information stored on, processed by, or transiting it</u> against unauthorized attempts to adversely <u>affect</u> their confidentiality, integrity, or availability.</p> <p>—</p> <p><i>Sharing:</i> “Providing, receiving, and disseminating.”</p> <p>—</p>	<p>occurrence and “reporting or recording” of an event are “as simultaneous as technologically and operationally practicable.”</p> <p><i>Security Control:</i> The management, operational, and technical controls used to protect an information system and its <u>information</u> against unauthorized attempts to adversely <u>impact</u> their <u>security</u>, confidentiality, integrity, or availability.</p> <p><i>Security Vulnerability:</i> “Any attribute of hardware, software, process, or procedure that could enable or facilitate the defeat of a security control.”</p> <p>—</p> <p><i>Tribal:</i> As in 25 U.S.C. 450b.</p> <p>—</p>	<p><i>Security Control:</i> The management, operational, and technical controls used to protect an information system and its <u>information</u> against unauthorized attempts to adversely <u>affect</u> their confidentiality, integrity, or availability.</p> <p>[Identical to PCNA]</p> <p>—</p> <p>[Identical to PCNA]</p> <p>—</p>
<p>(b) Amendment</p> <p>Adds tribal governments, private entities, and ISACs as appropriate members of the NCCIC in DHS.</p> <p>Sec. 203. Information Sharing Structure and Processes</p>	<p>Sec. 102. Sharing of Cyber Threat Indicators and Defensive Measures by the Federal Government With Non-federal Entities</p> <p>(a) In General</p>	<p>Sec. 3. Sharing of Information by the Federal Government</p> <p>(a) In General</p> <p>—</p>
<p>Amends Sec. 226 of the HSA.</p> <p>(I) 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</p>	<p>Amends Title I of the National Security Act of 1947 by adding a new section.</p> <p>‘Sec. 111. Sharing of Cyber Threat Indicators and Defensive Measures by the Federal Government With Non-Federal Entities’</p> <p>‘(a) Sharing by the Federal Government’</p> <p>‘(I)’ 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</p>	<p>Requires the DNI, <u>the Secretaries of Homeland Security and Defense, and the AG</u>, 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</p>

NCPAA	PCNA	CISA
<p>- providing information and recommendations on information sharing,</p>	<p>—</p>	<p>[Note: See also Sec. 5(c), p. 25, requiring DHS to implement the process for sharing electronic threat indicators and defensive measures with the federal government.]</p> <p>—</p>
<p>- in consultation with other appropriate agencies, collaborating with international partners, including on enhancing “the security and resilience of the global cybersecurity ecosystem,” and</p>	<p>—</p>	<p>—</p>
<p>- 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. 26.]</p>	<p>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.</p>	<p>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.</p>
<p>- notify the Secretary, the HSC, and the HSGAC of significant violations of privacy and civil liberties protections under ‘Sec. 226(i)(6),’</p>	<p>—</p>	<p>—</p>
<p>- promptly notifying nonfederal entities that have shared information known to be in error or in contravention to section requirements,</p>	<p>‘(2) Development of Procedures’ Requires that procedures for sharing developed by the DNI include methods to notify 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.</p>	<p>(b) Development of Procedures (1) requires that procedures for sharing developed by the DNI include methods to notify 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.</p>
<p>- participating in DHS-run exercises, and</p>	<p>—</p>	<p>—</p>
<p>—</p>	<p>Requires that the procedures incorporate existing information-sharing mechanisms of federal and nonfederal entities, including ISACs, as much as possible, and</p>	<p>[Identical to PCNA]</p>
<p>—</p>	<p>include methods to promote efficient granting of security clearances to appropriate representatives of</p>	<p>—</p>

NCPAA	PCNA	CISA
—	nonfederal entities.	—
(2) expands NCCIC membership to include the following [Note: all are existing entities]:	—	(2) requires that the procedures be developed in coordination with appropriate federal entities, including the National Laboratories, to ensure implementation of timely sharing of indicators.
- 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, 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		

NCPAA	PCNA	CISA
Requires that information be shared as appropriate with small and medium-sized businesses and that the NCCIC make self-assessment tools available to them,	<p>(f) Small Business Participation</p> <p>Requires the Small Business Administration to assist small businesses and financial institutions in monitoring, defensive measures, and sharing information under the section.</p>	—
—	<p>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.</p> <p>Requires federal outreach to those institutions to encourage them to exercise the authorities provided under the section.</p>	—
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 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. 24.]	(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	—	—

NCPAA	PCNA	CISA
<p>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</p> <ul style="list-style-type: none"> - 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. 		
<p>—</p>	<p>‘(b) Definitions’</p> <p>Defines the following terms by reference to Sec. 110 of the title: <i>Appropriate Federal Entities, Cyber Threat Indicator, Defensive Measure, Federal Entity, and Non-Federal Entity.</i></p>	<p>—</p>
<p>—</p>	<p>(b) Submittal to Congress</p> <p>Requires that the procedures developed by the DNI be submitted to Congress within <u>90</u> days of enactment of the title.</p>	<p>(c) Requires that the procedures developed by the DNI be submitted to Congress within <u>60</u> days of enactment of the bill.</p>
<p>—</p>	<p>(c) Table of Contents Amendment</p> <p>Revises the table of contents of the National Security Act of 1947 to reflect the addition of ‘Sec. 111.’</p>	<p>—</p>
<p>‘(i) Voluntary Information Sharing Procedures’</p>	<p>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</p> <p>(a) Requirement for Policies and Procedures</p> <p>(1) Adds new subsections to ‘Sec. 111’ of the National Security Act of 1947</p>	<p>Sec. 5. Sharing of Cyber Threat Indicators and Defensive Measures with the Federal Government</p> <p>(a) Requirement for Policies and Procedures</p> <p>—</p>
	<p>‘(b) Policies and Procedures for Sharing with the Appropriate Federal Entities Other Than the Department of Defense or the National Security Agency’</p>	

NCPAA	PCNA	CISA
<p>'(1)' permits voluntary information-sharing relationships for cybersecurity purposes between the NCCIC and nonfederal entities but prohibits requiring such an agreement.</p> <p>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).'</p> <p>Permits the Secretary, solely and unreviewably and acting through the U/S-CIP, to deny an agreement for national security reasons.</p>	<p>'(1)' requires the <u>President</u> to develop and submit to Congress policies and procedures for federal receipt of cyber threat indicators and defensive measures.</p>	<p>(1) requires the <u>AG</u>, in coordination with heads of <u>appropriate agencies</u>, to develop and submit to Congress policies and procedures for federal receipt of cyber threat indicators and defensive measures.</p>
<p>'(2)' permits the relationship to be established through a standard agreement for nonfederal entities not requiring specific terms.</p> <p>Stipulates negotiated agreements with DHS upon 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.</p>	<p>—</p>	<p>—</p>
<p>Stipulates that any agreement in effect prior to enactment of the title will be deemed in compliance with requirements in '(i).'</p> <p>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).'</p>	<p>—</p>	<p>—</p>
<p>—</p>	<p>'(2)' requires that the policies and procedures be <u>developed in accordance</u> with the privacy and civil liberties guidelines under Sec. 104(b) of the title, and ensure</p>	<p>(3) requires that, <u>consistent</u> with the privacy and civil liberties guidelines under Sec. (b), the policies and procedures ensure</p>
<p>—</p>	<p>- <u>real-time</u> sharing of indicators from <u>nonfederal entities</u> with <u>appropriate federal entities except DOD</u>,</p>	<p>- <u>automated</u> sharing of indicators from <u>any entity</u> with the <u>federal government</u> through the <u>real-time process</u> under (c),</p>
<p>—</p>	<p>- receipt without delay <u>except for good cause</u>, and</p>	<p>- <u>real-time</u> receipt without delay, with</p>

NCPAA	PCNA	CISA
—	- provision to all relevant federal entities,	- provision <u>permitted</u> 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 capability, and
—	- appropriate sanctions for federal personnel who knowingly and willfully <u>use shared information other than in accordance with the title.</u>	- appropriate sanctions for federal personnel who knowingly and willfully <u>conduct activities under the bill in an unauthorized manner.</u>
—	(2) requires that an interim version of the policies and procedures be submitted to Congress within <u>90</u> 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 <u>60</u> days of enactment of the title, and (2) the final version within 180 days.
—	—	(4) requires the AG 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 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 previously shared indicators and communications about cybersecurity threats by a regulated entity with its federal regulatory authority,
—	—	- ensure automated receipt by federal entities of

NCPAA	PCNA	CISA
—	—	indicators shared in real time with DHS,
—	—	- 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'		

NCPAA	PCNA	CISA
—	Establishes the CTIIC within the ODNI.	—
—	‘(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. 4(c) Authorization for Sharing or Receiving Cyber Threat Indicators or Defensive Measures
Permits nonfederal entities to share, for <u>cybersecurity</u> 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 <u>cybersecurity purposes and consistent with privacy requirements under (d)(2) and protection of classified information, lawfully obtained</u> cyber threat indicators or defensive measures	(1) permits entities to share, “for the purposes <u>permitted under this Act 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</u>	with any entity or the federal government,

NCPAA	PCNA	CISA
<p>notwithstanding any other provision of law, except that nonfederal recipients must comply with lawful restrictions on sharing and use imposed by the source.</p>	<p><u>entities except DOD.</u></p> <p>notwithstanding any other provision of law, (2) [Similar to NCPAA].</p>	<p>notwithstanding any other provision of law, (2) [Similar to NCPAA].</p>
<p>Requires <u>reasonable efforts</u> by nonfederal <u>and federal</u> entities, <u>prior to sharing</u>, to safeguard personally identifying information from unintended disclosure or unauthorized access or acquisition and remove <u>or exclude</u> such information where it is <u>reasonably believed when it is shared to be unrelated</u> to a cybersecurity <u>risk or incident</u>.</p>	<p>(d) Protection and Use of Information</p> <p>(2) requires <u>reasonable efforts by nonfederal</u> entities, <u>before sharing a threat indicator</u>, to</p> <p>—</p> <p>remove information <u>reasonably believed to be personal</u> or personally identifying of a specific person not <u>directly related</u> to a cybersecurity <u>threat</u>, or implement a technical capability for removing such information.</p>	<p>(d) Protection and Use of Information</p> <p>(2) requires entities, <u>before sharing a threat indicator</u>, to</p> <p>—</p> <p>remove information <u>known to be personal</u> or personally identifying of a specific person <u>not directly related</u> to a cybersecurity <u>threat</u>, or implement <u>and use</u> a technical capability for removing such information.</p>
<p>Sec. 109. Construction and Preemption</p> <p>(f) Information Sharing Relationships</p> <p>Stipulates that nothing in <u>'(3)'</u></p> <p>- limits or modifies an existing information sharing relationship or prohibits or requires a new one,</p>	<p>Sec. 109. Construction and Preemption</p> <p>(f) Information Sharing Relationships</p> <p>Stipulates that nothing in <u>the title</u></p> <p>- (1) limits or modifies an existing information sharing relationship or (2) prohibits or requires a new one.</p>	<p>Sec. 8. Construction and Preemption</p> <p>(f) Information Sharing Relationships</p> <p>Stipulates that nothing in <u>the bill</u></p> <p>[Similar to PCNA], or</p>
<p>—</p> <p>—</p> <p>—</p> <p>—</p>	<p>—</p> <p>Sec. 103(c)(3) stipulates that nothing in (c)</p> <p>- authorizes information sharing other than as provided in (c),</p> <p>- permits unauthorized sharing of classified information,</p> <p>- authorizes federal surveillance of any person,</p> <p>- prohibits a federal entity, at the request of a nonfederal entity, from technical discussion of threat</p>	<p>requires use of the DHS sharing process under Sec. 5(c) [p. 25].</p> <p>Sec. 4(c)(3) stipulates that nothing in (c)</p> <p>[Identical to PCNA]</p> <p>—</p>

NCPAA	PCNA	CISA
<p>- limits otherwise lawful activity, or</p> <p>- impacts or modifies existing procedures for reporting criminal activity to appropriate law enforcement authorities, or participating in an investigation.</p> <p>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.</p>	<p>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</p> <p>[Similar to NCPAA]</p> <p>—</p> <p>—</p>	<p>[Identical to PCNA]</p> <p>—</p> <p>—</p>
<p>‘(4) Network Awareness Authorization’</p> <p>permits <u>nonfederal, nongovernment</u> entities, notwithstanding any other provision of law, to <u>conduct network awareness</u>, for cybersecurity purposes and <u>to protect rights or property</u>, of</p> <p>- its own information systems,</p> <p>- with written consent, information systems of a nonfederal or federal entity, or</p> <p>- the contents of such systems.</p> <p>Stipulates that nothing in ‘(4)’</p> <p>- authorizes <u>network awareness</u> other than as provided in the <u>section</u>, or</p> <p>- limits otherwise lawful activity,</p> <p>—</p>	<p>(a) Authorization for Private-Sector Defensive Monitoring</p> <p>(1) permits <u>private</u> entities, notwithstanding any other provision of law, to <u>monitor</u>, for cybersecurity purposes,</p> <p>[Similar to NCPAA],</p> <p>[Similar to NCPAA], or</p> <p>[Similar to NCPAA].</p> <p>(2) Stipulates that nothing in (a)</p> <p>- authorizes <u>monitoring</u> other than as provided in the <u>title</u>,</p> <p>[Similar to NCPAA],</p> <p>- authorizes federal surveillance of any person.</p>	<p>(a) Authorization for Monitoring</p> <p>[Similar to PCNA],</p> <p>[Identical to PCNA],</p> <p>[Similar to NCPAA], or</p> <p>[Identical to PCNA].</p> <p>[Identical to NCPAA],</p> <p>[Similar to PCNA].</p> <p>—</p>
<p>‘(5) Defensive Measure Authorization’</p>	<p>(b) Authorization for Operation of Defensive Measures</p>	<p>(b) Authorization for Operation of Defensive Measures</p>

NCPAA	PCNA	CISA
<p>permits <u>nonfederal, nongovernment</u> entities to operate defensive measures, for cybersecurity purposes and to protect rights or property, that are <u>applied</u> to</p> <ul style="list-style-type: none"> - its own information systems, - with written <u>consent</u>, information systems of a <u>nonfederal or federal</u> entity, or 	<p>(1) permits <u>private</u> entities to operate defensive measures, for a cybersecurity purpose and to protect rights or property, that are <u>operated on</u></p> <p>[Similar to NCPAA], or</p> <ul style="list-style-type: none"> - with written <u>authorization</u>, information systems of a <u>nonfederal or federal</u> entity, or 	<p>(1) permits <u>private</u> entities to operate defensive measures, for cybersecurity purposes and to protect rights or property, that are <u>applied to</u></p> <p>[Similar to NCPAA]</p> <ul style="list-style-type: none"> - with written <u>consent</u>, information systems of <u>another</u> entity, or a <u>federal</u> entity with written <u>consent</u> of an authorized representative
<p>- the contents of such systems,</p> <p>notwithstanding any other provision of law, except that measures may not be used except as authorized in <u>the section</u>, and '(5)' does not limit otherwise lawful activity.</p>	<p>(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.</p>	<p>(1) notwithstanding any other provision of law, except (2) [Identical to PCNA].</p>
<p>[No Corresponding Provision; however, the definition of defensive measure in Sec. 202(a) includes a similar restriction; see p. 17.]</p>	<p>(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.</p>	<p>[No Corresponding Provision; however, the definition of defensive measure in Sec. 2 includes a similar restriction; see p. 17.]</p>
<p>—</p>	<p>(e) No Right or Benefit</p> <p>Stipulates that sharing of indicators with a nonfederal entity creates no right or benefit to similar information by any nonfederal entity.</p>	<p>(f) No Right or Benefit</p> <p>Stipulates that sharing of indicators with an entity creates no right or benefit to similar information by any entity. [Note: Definition of <i>entity</i> in CISA is similar to definition of <i>nonfederal entity</i> in PCNA; see p. 18.]</p>
<p>'(6) Privacy and Civil Liberties Protections'</p>	<p>Sec. 104(b) Privacy and Civil Liberties</p>	<p>Sec. 5(b) Privacy and Civil Liberties</p>
<p>Requires the <u>U/S-CIP</u>,</p> <p>in <u>coordination</u> with the DHS CPO and Chief Civil Rights and Civil Liberties Officer,</p> <p>to <u>establish</u> and review <u>annually</u> policies and procedures on <u>information shared</u> with the NCCIC under the</p>	<p>(1) requires the <u>AG</u>,</p> <p>in <u>consultation</u> with appropriate federal <u>agency heads</u> and agency privacy and civil liberties officers,</p> <p>to <u>develop</u> and review <u>periodically</u> guidelines on <u>privacy and civil liberties</u> to govern federal handling of cyber</p>	<p>(1) requires the <u>AG</u>,</p> <p>in <u>coordination</u> with appropriate federal <u>entity heads</u> and in <u>consultation</u> with agency privacy and civil liberties officers,</p> <p>to <u>develop interim</u> guidelines on <u>privacy and civil liberties</u> to govern federal handling of cyber threat</p>

NCPAA	PCNA	CISA
section.	threat indicators obtained through the title’s provisions.	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]	<p>(2) in <u>coordination</u> with appropriate federal <u>entity heads</u> and in <u>consultation</u> with agency privacy and civil liberties officers and <u>relevant private entities with industry expertise</u>, to <u>promulgate</u>, and review <u>periodically</u> in <u>coordination</u> with appropriate agency heads and <u>consultation</u> with agency privacy and civil liberties officers and relevant private entities, <u>final guidelines on privacy and civil liberties</u> to govern federal handling of cyber threat indicators obtained through the bill’s provisions</p>
Requires that they apply only to DHS, consistent with the need for <u>timely</u> protection of information systems from and mitigation of cybersecurity <u>risks and incidents</u> , the policies and procedures	(2) requires that, consistent with the need for protection of information systems and <u>threat</u> 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;
- “ <u>reasonably</u> limit, to the extent practicable, receipt, retention, use, and <u>disclosure</u> of cybersecurity threat indicators and defensive measures <u>associated with specific persons</u> ” not needed for timely protection of systems and networks,	- limit receipt, retention, use, and <u>dissemination</u> of cybersecurity threat indicators <u>containing personal information of or identifying specific persons</u> ,	(b)(3) [Similar to PCNA],
—	including by establishing processes for <u>prompt</u> destruction of information known not to be directly related to uses <u>for cybersecurity purposes</u> , setting limitations on retention of indicators, and notifying recipients that indicators may be used only for <u>cybersecurity purposes</u> , and,	including by establishing processes for <u>timely</u> destruction of information known not to be directly related to uses <u>under the title</u> , and setting limitations on retention of indicators, and requiring that recipients be informed that indicators may be used only for purposes <u>authorized under the bill</u> ,
- <u>minimize</u> impacts on privacy and civil liberties,	- <u>limit</u> impacts on privacy and civil liberties of federal activities under the title, including	- <u>limit</u> impacts on privacy and civil liberties of federal activities under the bill,

NCPAA	PCNA	CISA
<p>- provide data integrity through prompt removal and destruction of <u>obsolete or erroneous</u> personal information unrelated to the information shared and retained by the NCCIC in accordance with this section,</p>	<p>guidelines for removal of personal and personally identifying information handled by federal entities under the title,</p>	<p>—</p>
<p>- include requirements to safeguard from unauthorized access or acquisition cyber threat indicators and <u>defensive measures</u> retained by the NCCIC,</p>	<p>- include requirements to safeguard from unauthorized access or acquisition cyber threat indicators</p>	<p>[Identical to PCNA]</p>
<p>identifying specific persons, <u>including proprietary or business-sensitive information</u>,</p>	<p><u>containing personal information of</u> or identifying specific persons,</p>	<p>[Identical to PCNA]</p>
<p>- protect the confidentiality of cyber threat indicators and <u>defensive measures associated with specific persons</u>, to the greatest extent practicable,</p>	<p>—</p>	<p>- protect the confidentiality of cyber threat indicators <u>containing personal information of or identifying specific persons</u>, to the greatest extent practicable,</p>
<p>- ensure that relevant constitutional, legal, and privacy protections are observed.</p>	<p>- be consistent with other applicable provisions of law,</p>	<p>[See (a)(3), p. 31, stating that applicable provisions of law will govern information sharing activities, consistent with the bill],</p>
<p>—</p>	<p>- include procedures to notify entities if a federal entity receiving information knows that it is not a cyber threat indicator,</p>	<p>[Similar to PCNA],</p>
<p>—</p>	<p>- include steps to ensure that dissemination of indicators is consistent with the protection of classified and other sensitive national security information.</p>	<p>[Similar to PCNA].</p>
<p>Stipulates that the U/S-CIP may consult with NIST in developing the policies and procedures.</p>	<p>—</p>	<p>—</p>
<p>Requires the DHS CPO and the Officer for Civil Rights and Civil Liberties, in consultation with the PCLOB, to submit to appropriate congressional committees</p>	<p>(3) requires the AG to submit to Congress</p>	<p>Requires the AG to submit to Congress</p>
<p>the policies and procedures within 180 days of enactment and annually thereafter.</p>	<p>interim guidelines within <u>90</u> days of enactment and final guidelines within 180 days.</p>	<p>(1) interim guidelines within <u>60</u> days of enactment and (2) final guidelines within 180 days.</p>
<p>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.</p>	<p>—</p>	<p>(1) requires the AG to make the interim guidelines available to the public. [Note: There is no similar requirement for the final guidelines.]</p>

NCPAA	PCNA	CISA
<p>Requires the DHS CPO to</p> <ul style="list-style-type: none"> - 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. 	<p style="text-align: center;">—</p> <p>(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.]</p>	<p style="text-align: center;">—</p> <p>(b)(3) [Identical to PCNA]</p>
<p>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</p> <ul style="list-style-type: none"> - receipt, use, and dissemination of cybersecurity indicators and defensive measures shared with federal entities under the section, - information on NCCIC use of such information for purposes other than cybersecurity, - types of information shared with the NCCIC, - actions taken by NCCIC based on shared information; 	<p>Sec. 107. Oversight of Government Activities</p> <p>(b) Reports on Privacy and Civil Liberties.</p> <p>(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</p> <ul style="list-style-type: none"> - receipt, use, and dissemination of cybersecurity indicators and defensive measures shared with federal entities under the title, - types of indicators shared with federal entities, - actions taken by federal entities as a result of receiving 	<p>Sec. 7. Oversight of Government Activities</p> <p>(b) Reports on Privacy and Civil Liberties.</p> <p>(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</p> <p>[Similar to PCNA],</p> <p>[Identical to PCNA],</p> <p>[Identical to PCNA],</p>

NCPAA	PCNA	CISA
<p>- metrics to determine impacts of sharing on privacy and civil liberties,</p>	<p>shared <u>indicators</u>,</p>	<p>—</p>
<p>- a list of federal <u>agencies</u> receiving the <u>information</u>,</p> <p>- review of sharing of <u>information</u> within the federal <u>government</u> to identify inappropriate <u>stovepiping</u> of shared information, and</p>	<p>- a list of federal <u>entities</u> receiving the <u>indicators</u>,</p> <p>- review of sharing of <u>indicators</u> among federal <u>entities</u> to identify inappropriate <u>barriers</u> to sharing information,</p>	<p>[Identical to PCNA], and</p> <p>[Identical to PCNA].</p>
<p>—</p> <p>- recommendations for improvements or modifications to <u>sharing</u> under the <u>section</u>.</p>	<p>- procedures for sharing information and removal of personal and identifying information, and incidents involving improper treatment of it, and</p> <p>- recommendations for improvements or modifications to <u>authorities</u> under the <u>title</u>.</p>	<p>—</p> <p>(3) permits inclusion of recommendations for improvements or modifications to <u>authorities</u> under the <u>bill</u>.</p>
<p>—</p>	<p>Requires that the reports be submitted in unclassified form but permits a classified annex.</p>	<p>(4) [Similar to PCNA].</p>
<p>—</p>	<p>Requires public availability of unclassified parts of the reports.</p>	<p>—</p>
<p>—</p> <p>Requires the <u>DHS CPO and Chief Civil Rights and Civil Liberties Officer</u>, in consultation with the PCLOB, the DHS IG, and senior privacy and civil liberties officers of each federal agency receiving indicators or defensive measures shared with the NCCIC, to</p>	<p>(1) adds a new paragraph to Sec. 1061(e) of the Intelligence Reform and Terrorism Prevention Act of 2004:</p> <p>(3) requires the <u>PCLOB</u> to</p>	<p>—</p> <p>(1) [Similar to PCNA]</p>
<p>submit a biennial report to Congress</p> <p>assessing impacts on privacy and civil liberties of federal activities under '(6)', including</p>	<p>submit a biennial report to Congress and the President</p> <p>assessing <u>impacts</u> of activities under the title on and sufficiency of policies, procedures, and guidelines in addressing concerns about privacy and civil liberties, including</p>	<p>[Similar to PCNA]</p> <p>assessing <u>effects</u> of the <u>types</u> of activities under on the bill on and sufficiency of policies, procedures, and guidelines in addressing concerns about privacy and civil liberties.</p>
<p>recommendations to minimize or mitigate such impacts.</p>	<p>recommendations for improvements or modifications to authorities under the title.</p>	<p>(3) permits inclusion of recommendations for improvements or modifications to <u>authorities</u> under the</p>

NCPAA	PCNA	CISA
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.	<u>bill</u> , (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 and at least biennially thereafter, including
—	- review of types of indicators shared with the federal government,	[Similar to PCNA],
—	- 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,	[Identical to PCNA],
—	- 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. 5,
—	—	- effectiveness of real-time sharing under Sec. 5(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. 3 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	[Similar to PCNA],

NCPAA	PCNA	CISA
—	dissemination under the title,	
—	- 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) 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. 4. Authorizations for Preventing, Detecting, Analyzing, and Mitigating Cybersecurity Threats
[Nonfederal Entities]	(d) Protection and Use of Information	(d) Protection and Use of Information
Permits a nonfederal, <u>nongovernment</u> entity that shares indicators or defensive measures with the NCCIC to use, retain, or disclose indicators and defensive	(3) permits a nonfederal entity [Note: <u>including government entities</u>], for a cybersecurity purpose, to use an “indicator or defensive measure shared or received under this section to monitor or operate a	(3) permits an entity [Note: <u>including government entities</u>], for cybersecurity purposes, to use indicators or defensive measure shared or received under this section to monitor or operate a defensive

NCPAA	PCNA	CISA
measures, solely for cybersecurity purposes.	defensive measure on” its own information systems or those of other nonfederal or federal entities upon written <u>authorization</u> from them, with	measure on its own information systems or those of other entities upon written <u>consent</u> 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. 28, describing requirements for removal of personal information].	[See (2), p. 28, 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].
Stipulates that the information shall be deemed voluntarily shared.	—	—
Requires implementation <u>and utilization</u> of security controls to protect against unauthorized access or acquisition.	(1) requires implementation of <u>appropriate</u> security controls to protect against unauthorized access or acquisition. [Note: Also applies to nonfederal government entities.]	(1) Requires implementation <u>and utilization</u> 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 <u>other than as authorized in (d)</u> .
[Federal Entities]	Sec. 104(d) Information Shared with or Provided to the Federal Government	Sec. 5(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 cybersecurity purposes.	(5) permits federal entities <u>or personnel</u> receiving indicators or defensive measures under the title to, consistent with otherwise applicable provisions of federal law, use, retain, or disclose it solely for a cybersecurity purpose,	(5) [Similar to PCNA]
—	—	[Identical to PCNA] identifying a cybersecurity threat, - including a source or vulnerability, - use of an information system by a foreign adversary of terrorist,

NCPAA	PCNA	CISA
<p>[Note: Sec. 216 (see p. 53) permits use of information obtained from federal systems for <u>investigating</u>, <u>prosecuting</u>, <u>disrupting</u>, or otherwise responding to</p>	<p>“responding to, <u>investigating</u>, <u>prosecuting</u>, or otherwise <u>preventing or mitigating</u>”</p>	<p>“responding to or otherwise <u>preventing or mitigating</u>”</p>
<p>imminent threats of death or serious bodily harm</p>	<p>threats of death or serious bodily harm or offenses arising out of such threats,</p>	<p>imminent threats of death or serious bodily harm or</p>
<p>—</p>	<p>—</p>	<p>“serious economic harm, including a terrorist act or a use of a weapon of mass destruction,”</p>
<p>serious threats to minors, including sexual exploitation <u>or</u> threats to physical safety, and</p>	<p>“a serious threat to a minor, including sexual exploitation <u>and</u> threats to physical safety,” and</p>	<p>[Identical to PCNA],</p>
<p>violations of 18 U.S.C. 1030 [computer fraud], or</p>	<p>- 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, espionage and censorship, protection of trade secrets, and serious violent felonies].</p>	<p>[Similar to PCNA] or</p>
<p>—</p>	<p>—</p>	<p>—</p>
<p>attempts or conspiracy to commit the above offenses.]</p>	<p>Prohibits federal disclosure, retention, or use for any purpose not permitted under (5).</p>	<p>[Similar to PCNA].</p>
<p>—</p>	<p>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.</p>	<p>Stipulates that the policies, procedures, and guidelines in (a) and (b) apply to such information, that confidentiality of personal or personally identifying information in indicators must be protected and the information protected from unauthorized use or disclosure.</p>
<p>—</p>	<p>‘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 personally identifying of a specific person and to remove such information, or to implement a technical capability to remove <u>or exclude</u> such information.</p>	<p>Sec. 3(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 personally identifying of a specific person and to remove such information, or to implement <u>and utilize</u> a technical capability to remove such information.</p>
<p>Requires implementation and utilization of security controls to protect against unauthorized access or</p>	<p>‘Sec. 111(a)(2)’ requires that procedures for sharing developed by the DNI include requirements for federal</p>	<p>Sec. 3(b)(1) requires that procedures for sharing developed by the DNI include requirements for federal</p>

NCPAA	PCNA	CISA
acquisition.	entities to implement security controls to protect against unauthorized access to or acquisition of shared information.	entities to implement <u>and utilize</u> security controls to protect against unauthorized access to or acquisition of shared information.
Prohibits use in surveillance or collection activities to track an individual’s personally identifiable information except as authorized in the section.	Sec. 109(a) Prohibition of 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.	Stipulates that the title does not authorize DOD or any element of the IC to target a person for surveillance.	Sec. 5(d)(3) stipulates that indicators and defensive measure provided to the federal government under the bill shall be deemed voluntarily shared information..
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).	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.	[Similar to PCNA].
_____	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),	_____
Prohibits federal use for regulatory purposes.	except for information requiring disclosure in criminal prosecutions.	(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 bill.
Specifies that there is no waiver of applicable privilege or protection under law, including trade-secret protection;	[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.]	(1) [Similar to NCPAA].
Requires that the information be considered the commercial, financial, and proprietary information of the <u>nonfederal entity</u> when so designated by it.	(1) [Similar to NCPAA].	(2) requires that, consistent with <u>Sec. 4(c)(2)</u> , the information be considered the commercial, financial, and proprietary information of the <u>entity providing it</u> , when so designated by the <u>originating entity</u> or <u>third party</u> acting with written authorization from it.
	(2) requires that, consistent with the <u>title</u> , the information be considered the commercial, financial, and proprietary information of the originating <u>nonfederal source</u> , when so designated by <u>such source</u> or <u>nonfederal entity</u> acting with written authorization from it.	

NCPAA	PCNA	CISA
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. 36.]	[Note: See also Nonfederal Entities, p. 36.]
Permits state, local, and tribal government to use, retain, or further disclose indicators <u>or defensive measures</u> shared under the section solely for.	Sec. 103(d)(4) permits state, local, and tribal government entities	Sec. 4(d)(4) permits state, local, and tribal government entities, <u>with prior written consent of sharing entity or oral consent in exigent circumstances.</u>
cybersecurity purposes.	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. 5(d)(5)]
_____	a cybersecurity purpose,	investigating, prosecuting, or preventing
_____	“responding to, investigating, prosecuting, 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.”	_____
_____	_____	_____
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. 28, describing requirements for removal of personal information.]	offenses relating to serious violent felonies, 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.]
Stipulates that the information be considered “commercial, financial, and proprietary” if so designated by the provider.	[See (2), p. 28, 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. 36.]	[Similar to PCNA].

NCPAA	PCNA	CISA
Stipulates that the indicators and <u>defensive measures</u> shall be deemed voluntarily shared.	Stipulates that such shared indicators or <u>defensive measures</u> 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 <u>and utilization</u> of security controls to protect against unauthorized access or acquisition.	(1) requires implementation of <u>appropriate</u> security controls to protect against unauthorized access or acquisition. [Note: Also applies to nonfederal nongovernment entities.]	(1) Requires implementation <u>and utilization</u> 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.
Prohibits use for regulation of lawful activities of nonfederal entities.	—	Prohibits 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.
‘(8) Liability Exemptions’	Sec. 106. Protection from Liability	Sec. 6. Protection from Liability
States that “no cause of action shall lie or be maintained in any court” against <u>nonfederal, nongovernment</u> entities for <u>conducting network awareness</u> under ‘(4)’ in accordance with the <u>section</u> or	(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 <u>private</u> entities for <u>monitoring information systems</u> under Sec. 103(a) conducted in accordance with the <u>title</u> or	[Similar to PCNA, but refers to Sec. 4(a)]
for sharing indicators or defensive measures under ‘(3),’ or a <u>good-faith failure</u> to act if sharing is done in accordance with the <u>section</u> .	(b) Sharing or Receipt of Cyber Threat Indicators	(b) Sharing or Receipt of Cyber Threat Indicators
	for information sharing under Sec. 103(c) in accordance with the title or a <u>good-faith failure</u> to act if sharing is done in accordance with the <u>title</u> .	for information sharing under Sec. 4(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. 5(a)(1) or 60 days after enactment, it uses the DHS process under Sec. 5(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

NCPAA	PCNA	CISA
- requires dismissal of a cause of action against a nonfederal, nongovernment entity that engages in willful misconduct in the course of activities under the <u>section</u> .	requires dismissal of a cause of action against a nonfederal entity that engages in willful misconduct in the course of activities under the <u>title</u> , or	- requires dismissal of a cause of action against an entity that engages in <u>gross negligence or</u> willful misconduct in the course of activities under the <u>bill</u> , or
- undermines or limits availability of otherwise applicable common law or statutory defenses.	[Identical to NCPAA]	[Identical to NCPAA]
Establishes the burden of proof as clear and convincing evidence from the plaintiff of injury-causing willful misconduct,	(2) [Similar to NCPAA]	—
Defines <i>willful misconduct</i> 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 <u>restrictions on federal disclosure and use under ‘Sec. 226’</u> , with minimum damages of \$1,000 plus	Makes the federal government liable to injured persons for intentional or willful violation of <u>privacy and civil liberties guidelines under Sec. 104(b)</u> , 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 <u>disclosed the information</u> is located.	where the federal department or agency that <u>violated the guidelines</u> is located.	—
	(c) Statute of Limitations	

NCPAA	PCNA	CISA
Sets the statute of limitations under <u>'(i)'</u> at two years from the date on which the cause of action arises.	Sets the statute of limitations under <u>Sec. 105</u> at two years from the date on which the cause of action arises.	—
Sets action under <u>'(i)'</u> as the exclusive remedy for violation of <u>restrictions under '(i)(3), '(i)(6), or '(i)(7)(B)'</u> .	(d) Exclusive Cause of Action. Sets action under (d) as the exclusive remedy for federal violations under <u>the title</u> .	—
'(10) Anti-Trust 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.	—	Sec. 4(e) Antitrust Exemption Exempts any two or more private entities from violation of antitrust laws, except as provided in Sec. 8(e) [p. 44] 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' Stipulates that the <u>section</u> does not limit or prohibit otherwise lawful disclosures <u>or participation in an investigation</u> by a nonfederal entity of information to any other federal or nonfederal entity.	Sec. 109(b) Otherwise Lawful Disclosures Stipulates that the <u>title</u> does not limit or prohibit otherwise lawful disclosures by a nonfederal entity of information to any other federal or nonfederal entity, or any otherwise lawful use by a federal entity, <u>whether or not</u> the disclosures duplicate those made under the title.	Sec. 8(a) Otherwise Lawful Disclosures Stipulates that the <u>bill</u> does not limit or prohibit otherwise lawful disclosures by an entity of information to any federal or other entity, or any otherwise lawful use by a federal entity, <u>even when</u> the disclosures duplicate those made under the bill.
— Stipulates that the <u>section</u> does not prohibit or limit disclosures protected under 5 U.S.C. 2302(b)(8), 5 U.S.C. 7211, 10 U.S.C. 1034, <u>50 U.S.C. 3234</u> , or similar provisions of federal or state law.	(c) Whistle Blower Protections Stipulates that the <u>title</u> does not 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.	(b) Whistle Blower Protections Stipulates that the <u>bill</u> does not prohibit or limit disclosures protected under 5 U.S.C. 2302(b)(8), 5 U.S.C. 7211, 10 U.S.C. 1034, <u>50 U.S.C. 3234</u> , or similar provisions of federal or state law.
Stipulates that the <u>section</u> does not affect any requirements under other provisions of law for nonfederal entities providing information to federal entities.	(e) Relationship to Other Laws Stipulates that the <u>title</u> does not affect any requirements under other provisions of law for nonfederal entities providing information to federal entities.	Stipulates that the <u>bill</u> does not affect any requirements under other provisions of law for entities providing information to federal entities.

NCPAA	PCNA	CISA
<p>Stipulates that the <u>section</u> does not change contractual relationships between nonfederal entities or them and federal entities or abrogate trade-secret or intellectual property rights.</p> <p>Stipulates that the <u>section</u> does not permit the federal government to require nonfederal entities to provide it with information, or</p> <p>condition sharing of indicators or <u>defensive measures</u> on provision by such entities of indicators or defensive measures, or</p> <p>condition award of grants, contracts, or purchases on such provision.</p> <p>Stipulates that the <u>section</u> does not create liabilities for any nonfederal entities that choose not to engage in the voluntary activities authorized in the <u>section</u>.</p> <p>Stipulates that the <u>section</u> does not authorize or modify existing federal authority to retain and use information shared under the title for uses other than those permitted under the <u>section</u>.</p> <p>Stipulates that the section does not restrict or condition sharing for cybersecurity purposes among nonfederal entities or require sharing by them with the NCCIC.</p> <p>Stipulates that nothing in the bill “<u>shall</u> be construed to permit price-fixing, allocating a market between competitors, monopolizing or attempting to monopolize</p>	<p>(g) Preservation of Contractual Obligations and Rights</p> <p>Stipulates that the <u>title</u> does not change contractual relationships between nonfederal entities or them and federal entities, or abrogate trade-secret or intellectual property rights.</p> <p>(h) Anti-Tasking Restriction</p> <p>Stipulates that the <u>title</u> does not permit the federal government to require nonfederal entities to provide it with information, or</p> <p>condition sharing of indicators on provision of indicators, or</p> <p>condition award of grants, contracts, or purchases on such provision.</p> <p>(i) No Liability for Non-Participation</p> <p>Stipulates that the <u>title</u> does not create liabilities for any nonfederal entities that choose not to engage in a voluntary activity authorized in the <u>title</u>.</p> <p>(j) Use and Retention of Information</p> <p>Stipulates that the <u>title</u> does not authorize or modify existing federal authority to retain and use information shared under the title for uses other than those permitted under the <u>title</u>.</p> <p>—</p> <p>—</p>	<p>(g) Preservation of Contractual Obligations and Rights</p> <p>Stipulates that the <u>bill</u> does not change contractual relationships between entities or them and federal entities, or abrogate trade-secret or intellectual property rights.</p> <p>(h) Anti-Tasking Restriction</p> <p>Stipulates that the <u>bill</u> does not permit the federal government to require nonfederal entities to provide it with information, or</p> <p>[Similar to PCNA]</p> <p>[Identical to PCNA]</p> <p>(i) No Liability for Non-Participation</p> <p>Stipulates that the <u>bill</u> does not create liabilities for any nonfederal entities that choose not to engage in the voluntary activities authorized in the <u>bill</u>.</p> <p>(j) Use and Retention of Information</p> <p>Stipulates that the <u>bill</u> does not authorize or modify existing federal authority to retain and use information shared under the title for uses other than those permitted under the <u>bill</u>.</p> <p>—</p> <p>(e) Prohibited Conduct</p> <p>Stipulates that nothing in the bill “<u>may</u> be construed to permit price-fixing, allocating a market between competitors, monopolizing or attempting to monopolize</p>

NCPAA	PCNA	CISA
a market, <u>boycotting</u> , or exchanges of price or cost information, customer lists, or information regarding future competitive planning.”		a market, boycotting, or exchanges of price or cost information, customer lists, or information regarding future competitive planning.”
Specifies that the <u>section</u> supersedes state and local laws relating to its provisions	(k) Federal Preemption (1) Specifies that the <u>title</u> supersedes state and local laws relating to its provisions.	(k) Federal Preemption (1) Specifies that the <u>bill</u> 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.	_____	_____
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.	_____	_____
_____	(d) Protection of Sources and Methods Stipulates that the title does not affect federal enforcement actions on classified information or conduct of authorized law-enforcement or intelligence activities, or modify the authority of <u>the President or</u>	(c) Protection of Sources and Methods Stipulates that the bill does not affect federal enforcement actions on classified information or conduct of authorized law-enforcement or intelligence activities, or modify the authority of federal entities to

NCPAA	PCNA	CISA
	<p>federal entities to protect <u>and control dissemination of</u> classified information, <u>intelligence</u> sources and methods, and U.S. national security.</p>	<p>protect classified information, sources and methods, and U.S. national security.</p> <p>(m) Authority of Secretary of Defense to Respond to Cyber Attacks</p> <p>Stipulates that the bill does not “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.”</p>
<p>Sec. 204. Information Sharing and Analysis Organizations</p>		
<p>Amends Sec. 212 of the HSA to</p>	<p>—</p>	<p>—</p>
<p>(1) broaden the functions of ISAOs to include cybersecurity risk and incident information beyond that relating to critical infrastructure, and</p>	<p>—</p>	<p>—</p>
<p>(2) add by reference the definitions of <i>cybersecurity risk</i> and <i>incident</i> in 6 U.S.C. 148(a).</p>	<p>—</p>	<p>—</p>
<p>Sec. 205. Streamlining of Department of Homeland Security Cybersecurity and Infrastructure Protection Organization</p>		
<p>(a) Cybersecurity and Infrastructure Protection Directorate</p>		
<p>Renames the DHS National Protection and Programs Directorate as the Cybersecurity and Infrastructure Protection. [Sic.]</p>	<p>—</p>	<p>—</p>
<p>(b) Senior Leadership of the Cybersecurity and Infrastructure Protection Directorate</p>		
<p>Provides a specific title for the undersecretary in charge of critical infrastructure protection as U/S-CIP. Also</p>	<p>—</p>	<p>—</p>

NCPAA	PCNA	CISA
<p>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.</p>		
<p>(c) Report</p>		
<p>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.</p>	<p>—</p>	<p>—</p>
<p>Sec. 206. Cyber Incident Response Plans</p>		
<p>(a) In General</p>		
<p>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:</p>	<p>—</p>	<p>—</p>
<p>‘(b) Updates to the Cyber Incident Annex to the National Response Framework’</p>		
<p>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.</p>	<p>—</p>	<p>—</p>
<p>(b) Clerical Amendment</p>		
<p>Amends the table of contents of the act to reflect the title change made by (a).</p>	<p>—</p>	<p>—</p>

NCPAA	PCNA	CISA
<p>Sec. 207. Security and Resiliency of Public Safety Communications; Cybersecurity Awareness Campaign</p>		
<p>(a) In General</p>		
<p>Adds two new sections to the HSA:</p>	<p>—</p>	<p>—</p>
<p>‘Sec. 230. Security and Resiliency of Public Safety Communications’</p>		
<p>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.</p>	<p>—</p>	<p>—</p>
<p>‘Sec. 231. Cybersecurity Awareness Campaign’</p>		
<p>‘(a) In General’</p>		
<p>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.</p>	<p>—</p>	<p>—</p>
<p>‘(b) Consultation’</p>		
<p>Requires consultation with a wide range of stakeholders.</p>	<p>—</p>	<p>—</p>
<p>‘Sec. 232. National Cybersecurity Preparedness Consortium’</p>		
<p>‘(a) In General’</p>		
<p>Authorizes the Secretary to establish the National Cybersecurity Preparedness Consortium to</p>	<p>—</p>	<p>—</p>
<p>‘(b) Functions’</p>		
<p>- provide cybersecurity training to state and local first responders and officials, - establish a training curriculum for them using the DHS</p>	<p>—</p>	<p>—</p>

NCPAA	PCNA	CISA
<p>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.</p>		
‘(c) Members’		
<p>Stipulates that members be academic, nonprofit, and government partners with prior experience conducting cybersecurity training and exercises in support of homeland security.</p>	—	—
(b) Clerical Amendment		
<p>Amends the table of contents of the act to include the new sections.</p>	—	—
Sec. 208. Critical Infrastructure Protection Research and Development		
(a) Strategic Plan; Public-Private Consortiums		
<p>Adds a new section to the HSA:</p>	—	—
‘Sec. 318. Research and Development Strategy for Critical Infrastructure Protection’		
‘(a) In General’		
<p>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.</p>	—	—
‘(b) Contents of Plan’		
<p>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</p>	—	—

NCPAA	PCNA	CISA
<p>technologies to address rapidly evolving threats and technology and including clearly defined roadmaps,</p> <ul style="list-style-type: none"> - 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. 		
<p>‘(c) Coordination’</p>		
<p>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.]</p>	<p>—</p>	<p>—</p>
<p>‘(d) Consultation’</p>		
<p>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.</p>	<p>—</p>	<p>—</p>
<p>(b) Clerical Amendment</p>		
<p>Amends the table of contents of the act to include the new section.</p>	<p>—</p>	<p>—</p>
<p>Sec. 209. Report on Reducing Cybersecurity Risks in DHS Data Centers</p>		
<p>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.</p>	<p>—</p>	<p>—</p>
<p>—</p>	<p>Sec. 108. Report on Cybersecurity Threats</p> <p>(a) Report Required</p> <p>Requires the DNI, in <u>consultation</u> with heads of other appropriate elements of the IC, to submit within 180 days of enactment a report to the House and Senate</p>	<p>Sec. 9. Report on Cybersecurity Threats</p> <p>(a) Report Required</p> <p>Requires the DNI, in <u>coordination</u> with heads of other appropriate elements of the IC, to submit within 180 days of enactment a report to the House and Senate</p>

NCPAA	PCNA	CISA
	Intelligence Committees on cybersecurity threats <u>to the U.S. national security and economy</u> , including attacks, theft, and data breaches.	Intelligence Committees on cybersecurity threats, including attacks, theft, and data breaches.
	(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, <u>specifically</u> 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	
—	Requires that the report be unclassified, but may include a classified <u>annex</u> .	Requires that the report be made available in unclassified and classified <u>forms</u> .
	(d) Public Availability of Report	
—	Requires that the unclassified portion of the report be publicly available.	—
	(e) Intelligence Community Defined	(d) Intelligence Community Defined

NCPAA	PCNA	CISA
—	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. 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.	—	—
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.	—	—
Sec. 213. Prohibition on New Regulatory Authority	Sec. 109(I) Regulatory Authority	Sec. 8(I) 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 bill 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		

NCPAA	PCNA	CISA
Systems		
(a) In General		
Adds a new section to the HSA.	—	—
'Sec. 233. Available Protection of Federal Information Systems'		
'(a) In General'		
Requires the Secretary to make available to agencies capabilities, including technologies for continuous diagnostics and mitigation, for protecting federal information systems and their contents from risks.	—	—
'(b) Activities'		
Authorizes the Secretary to	—	—
- access information on a 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,	—	—
- obtain assistance through agreements or otherwise from private entities for implementing technologies under '(a),'	—	—
- use, retain, and disclose information obtained under this section only to protect federal systems and their contents 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. 38).]	[Note: Sec. 5(d)(5) has related provisions for information shared with the federal government (see p. 38).]
'(c) Conditions'		

NCPAA	PCNA	CISA
Requires that the agreements bar disclosure of identifying information reasonably believed to be unrelated to a cybersecurity risk except to DHS or the disclosing agency, or use of information accessed under the section by a private entity for any purpose other than protecting federal information systems and their contents or administration of the agreement.	—	—
‘(d) Limitation’		
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).’	—	—
(b) Clerical Amendment		
Amends the table of contents of the act to include the new section.	—	—
Sec. 217. Sunset	Sec. 112. Sunset	
Terminates the provisions in the title seven years after enactment.	[Identical to NCPAA]	—
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.	—	—
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	—	—

NCPAA	PCNA	CISA
and construction, enhanced modeling of impacts from incidents or threats, and facilitating incentivization of investments to strengthen cybersecurity and resilience of CI.		
Sec. 220. GAO Report on Impact Privacy and Civil Liberties	Sec. 111. Comptroller General Report on Removal of Personal Identifying Information	
Requires a report from the Comptroller General to HSC and HSGAC within five years of enactment assessing the impacts of NCCIC activities on privacy and civil liberties.	(a) Report Requires a report from the Comptroller General 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. 10. Conforming Amendments
—		(a) Public Information Amends 5 U.S.C. 552(b) [on public information] to specify protection from federal disclosure of information provided under the bill.
		(b) Modification of Limitation on Dissemination of Certain Information Concerning Penetrations of Defense Contractor Networks 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 procedures promulgated by the AG under Sec. 5 of the bill.

Source: CRS.

Notes: See “Notes on the Table.”

Author Contact Information

Eric A. Fischer
Senior Specialist in Science and Technology
efischer@crs.loc.gov, 7-7071

Stephanie M. Logan
Research Assistant
slogan@crs.loc.gov, 7-0504