Congressional Research Service
Informing the legislative debate since 1914

Cybersecurity and Information Sharing: Comparison of H.R. 1560 and H.R. 1731 as Passed by the House

Eric A. Fischer
Senior Specialist in Science and Technology

April 29, 2015

Congressional Research Service
7-5700
www.crs.gov
R43996

CRS REPORT
Prepared for Members and
Committees of Congress

Summary

Effective sharing of information in cybersecurity is generally considered an important tool for protecting information systems and their contents from unauthorized access by cybercriminals and other adversaries. 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. The White House has also submitted a legislative proposal and issued an executive order on the topic.

In the House, H.R. 1560, the Protecting Cyber Networks Act (PCNA), was reported out of the Intelligence Committee. H.R. 1731, the National Cybersecurity Protection Advancement Act of 2015 (NCPAA), was reported by the Homeland Security Committee. Both bills passed the House, amended, the week of April 20, and were combined, with the PCNA becoming Title I and the NCPAA Title II of H.R. 1560.

The PCNA and the NCPAA have many similarities but also significant differences. Both 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 both address some other topics in common.

The NCPAA would amend portions of the Homeland Security Act of 2002, and the PCNA would amend parts of the National Security Act of 1947. They differ in how they define some terms in common such as cyber threat indicator, the roles they provide for federal agencies (especially, the Department of Homeland Security and the intelligence community), 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.

S. 754 has been reported by the Senate Intelligence Committee. Presumably, if the Senate passes a bill on information sharing, any inconsistencies between the PCNA and the NCPAA could be reconciled during the process for resolving differences between the House and Senate bills.

All of the bills would address commonly raised concerns about barriers to sharing information about threats, attacks, vulnerabilities, and other aspects of cybersecurity—both within and across sectors. Such barriers are considered by many to hinder protection of information systems, especially those associated with critical infrastructure. Private-sector entities often claim that they are reluctant to share such information among themselves because of concerns about legal liability, antitrust violations, 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 that might arise from such sharing. While reduction or removal of such barriers may provide benefits, concerns have also been raised about potential adverse impacts, especially on privacy and civil liberties, and potential misuse of shared information. The legislative proposals all address many of the concerns. In general, the proposals 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 the proposals 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 two additional factors in particular may be worthy of consideration as the various legislative proposals are debated. First, resistance to sharing of information among private-sector entities might not be substantially reduced by the actions contemplated in the legislation. Second, information sharing is only one of many facets of cybersecurity that organizations need to address to secure their systems and information.

Contents

Tables

Contacts

This report compares provisions in two bills in the House of Representatives that address information sharing and related activities in cybersecurity:[1]

- H.R. 1560, the Protecting Cyber Networks Act (PCNA), as reported by the House Permanent Select Committee on Intelligence on April 13; and
- H.R. 1731, the National Cybersecurity Protection Advancement Act of 2015 (NCPAA), as ordered reported by the Committee on Homeland Security on April 14.[2]

Both 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 both address some other topics in common. In addition to other provisions, the NCPAA would explicitly amend portions of the Homeland Security Act of 2002 (6 U.S.C. 101 et seq.), and the PCNA would amend parts of the National Security Act of 1947 (50 U.S.C. 3021 et seq.).

This report consists of an overview of those and other legislative proposals on information sharing, along with selected associated issues, followed by a side-by-side analysis of the two House bills as passed. 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.

House Consideration of the Two Bills

The House Committee on Rules held a hearing on proposed amendments to both H.R. 1560 and H.R 1731 on April 21. More than 30 amendments were submitted for H.R. 1731 and more than 20 for H.R. 1560.[3] 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 H.R. 1560 and 11 for H.R. 1731. For each bill, a manager's amendment would serve as the base bill for floor consideration, with debate on H.R. 1560 held on April 22 and on H.R. 1731 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

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

[2] The Rules Committee print is available at http://docs.house.gov/billsthisweek/20150420/CPRT-114-HPRT-RU00-HR1731.pdf.

[3] 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.

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 the PCNA Title I and the NCPAA Title II.

Current Legislative Proposals

Five bills on information sharing have been introduced in the 114th Congress, three in the House and two in the Senate. The White House has also submitted a legislative proposal[4] (WHP) and issued an executive order on the topic.[5] Other proposals include the following:

- The Cyber Intelligence Sharing and Protection Act (CISPA), which passed the House in the 113th Congress, has been reintroduced as H.R. 234.
- S. 456 is an amended version of the White House proposal.[6]
- S. 754, the Cybersecurity Information Sharing Act of 2015 (CISA), from the Senate Intelligence Committee, has many similarities to a bill with the same name introduced in the 113th Congress and shares many provisions with the PCNA, although there are also significant differences between S. 754 and the PCNA.

All the bills would address concerns that are commonly raised about barriers to sharing of information on threats, attacks, vulnerabilities, and other aspects of cybersecurity—both within and across sectors. It is generally recognized that effective sharing of information is an important tool in the protection of information systems and their contents from unauthorized access by cybercriminals and other adversaries.

Barriers to sharing have long been considered by many to be a significant hindrance to effective protection of information systems, especially those associated with critical infrastructure.[7] Private-sector entities often claim that they are reluctant to share such information among themselves because of concerns about legal liability, antitrust violations, 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. While reduction or removal of such barriers may provide benefits in cybersecurity, concerns have also been raised

[4] 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.

[5] Executive Order 13691, "Promoting Private Sector Cybersecurity Information Sharing," *Federal Register* 80, no. 34 (February 20, 2015): 9349–53, http://www.gpo.gov/fdsys/pkg/FR-2015-02-20/pdf/2015-03714.pdf.

[6] See Senate Committee on Homeland Security and Government 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.

[7] 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.

about potential adverse impacts, especially with respect to privacy and civil liberties, and potential misuse of shared information.

The legislative proposals all address many of those concerns, but they vary somewhat in emphasis and method. The NCPAA focuses on the role of the Department of Homeland Security (DHS), and in particular the National Cybersecurity and Communications Integration Center (NCCIC). The PCNA, in contrast, focuses on the role of the intelligence community (IC),[8] including authorization of the recently announced Cyber Threat Intelligence Integration Center (CTIIC). Both CISPA and CISA address roles of both DHS and the IC. The NCPAA, S. 456, and the WHP address roles of information sharing and analysis organizations (ISAOs).[9] ISAOs were defined in the Homeland Security Act (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 also be ISAOs but are not the same, having been originally formed pursuant to a 1998 presidential directive.[10]

On April 21, the White House announced support for passage of the NCPAA, while calling for a narrowing of sweep for the liability protections, clarification of provisions on use of shared information in federal law enforcement, and additional safeguards relating to use of defensive measures.[11] The White House did not support passage of the PCNA without changes to its privacy and civil liberties provisions, the sweep of its liability protections, antitrust provisions, and safeguards on use of defensive measures.[12]

All of the proposals have provisions aimed at facilitating sharing of information among private-sector entities and providing protections from liability that might arise from such sharing. They vary somewhat in the kinds of private-sector entities and information covered, but almost all of them address information on both cybersecurity threats and defensive measures, the exception being S. 456 and the WHP, which cover only cyber threat indicators. In general, the proposals limit the use of shared information to purposes of cybersecurity and law enforcement, and they limit government use, especially for regulatory purposes.

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

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

[9] 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).

[10] The White House, "Presidential Decision Directive 63: Critical Infrastructure Protection," May 22, 1998, http://www.fas.org/irp/offdocs/pdd/pdd-63.htm.

[11] 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.

[12] 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.

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).

H.R. 1735, the National Defense Authorization Act of 2016, as ordered reported by the House Armed Services Committee on April 30, would provide liability protections similar to those in H.R. 1560 to "operationally critical" defense contractors who are required to report incidents to DOD (10 U.S.C. 391) and cleared contractors required to report network or system penetrations (10 U.S.C. 2224 note).

While most observers appear to believe that legislation on information sharing is either necessary or at least potentially beneficial—provided that appropriate protections are included—two additional factors in particular may be worthy of consideration as the legislative proposals are developed. First, resistance to sharing of information among private-sector entities might not be substantially reduced by the actions contemplated in the legislation. Information received can help an entity prevent or mitigate an attack. However, there is no clear direct benefit associated with providing information, except in the case of providers of cybersecurity services and their clients. More indirect benefits might occur, for example, if a pattern of reciprocity develops among sharing entities, such as through ISACs or ISAOs. While the legislative proposals 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 that asymmetry, the degree to which information sharing will increase under the provisions of the various legislative proposals may be uncertain.

The second point is that information sharing is only one of many facets of cybersecurity.[13] Entities must have the resources and processes in place that are necessary for effective cybersecurity risk management. Sharing may be relatively unimportant for many organizations, especially in comparison with other cybersecurity needs.[14] In addition, most information sharing relates to imminent or near-term threats. It is not directly relevant to broader issues in cybersecurity such as education and training, workforce, acquisition, or cybercrime law, or major long-term challenges such as building security into the design of hardware and software, changing the incentive structure for cybersecurity, developing a broad consensus about cybersecurity needs and requirements, and adapting to the rapid evolution of cyberspace.

[13] See, for example, Testimony of Martin C. Libicki before the House Committee on Oversight & 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.

[14] 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).

Comparison of the NCPAA and the PCNA

The remainder of the report consists of a side-by-side comparison of provisions in H.R. 1560 and H.R. 1731 as passed by the House and combined as separate titles into a single bill, H.R. 1560. The PCNA became Title I and the NCPAA became Title II.

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
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 the NCPAA serving as the basis for comparison.[15] As a result, many provisions of the 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 the 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. 15, 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 the report.
- Explanatory notes on provisions are enclosed in square brackets. Also, the entry "[Similar to NCPAA]" means that the text in that provision in the PCNA is closely similar in text, with no significant difference in meaning, to the corresponding provision in the NCPAA. "[Identical to NCPAA]" means that there are no differences in language in the two provisions.

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

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

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

NCPAA—Title II	PCNA—Title I
"To amend the Homeland Security Act of 2002 to enhance multi-directional sharing of information related to cyber-security risks and strengthen privacy and civil liberties protections, and for other purposes."	"To improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes." [*Note:* These two official titles have been concatenated in the engrossed version of H.R. 1560.]
Sec. 201. Short Title	**Sec. 101. Short Title**
National Cybersecurity Protection Advancement Act of 2015	Protecting Cyber Networks Act
Sec. 202. National Cybersecurity and Communications Integration Center	
Amends Sec. 226 of the HSA (6 U.S.C. 148). [*Note:* This section, added by P.L. 113-282, established the National Cybersecurity and Communications Integration Center and is referred to in the bill as the "second section 226" to distinguish it from an identically numbered section added by P.L. 113-277.]	
(a) In General	**Sec. 110. Definitions**
Amends existing definitions:	
Cybersecurity Risk: Excludes actions solely involving violations of consumer terms of service or licensing agreements from the definition.	
Incident: Replaces the phrase "or actually or imminently jeopardizes, without lawful authority, an information system" with "or constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies."	
Adds the following definitions:	
	Agency: As in 44 U.S.C. 3502.
	Appropriate Federal Entities: Departments of Commerce, Defense, Energy, Homeland Security, Justice, and the Treasury; and Office of the ODNI.
	Cybersecurity Threat: An action unprotected by the 1st Amendment to the Constitution that involves an information system and may result in unauthorized efforts to adversely impact the security, integrity, confidentiality, or availability of the system or its contents, but not including actions solely involving violations of consumer terms of service or licensing agreements.
Cyber Threat Indicator: Technical information necessary to describe or identify	*Cyber Threat Indicator:* Information or a physical object necessary to describe or identify
- a method for 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, including
- communications that reasonably appear to have "the purpose of gathering technical information related to a cybersecurity risk,"	- anomalous patterns of communications that appear to have "the purpose of gathering technical information related to a cybersecurity threat or security vulnerability,"

NCPAA—Title II	PCNA—Title I
- a method for defeating a technical or security control,	- a method of defeating a security control or exploiting a security vulnerability,
- a technical vulnerability including anomalous technical behavior that may become a vulnerability,	- a security vulnerability or anomalous activity indicating the existence of one,
- a method of causing a legitimate user of an information system or its contents to inadvertently enable defeat of a technical or operational control,	- a method of causing a legitimate user of an information system or its contents to unwittingly enable defeat of a security control or exploitation of a security vulnerability,
- a method for unauthorized remote identification, access, or use of an information system or its contents, if the method is known or reasonably suspected of association with a known or suspected cybersecurity risk, or	- "malicious cyber command and control,"
- actual or potential harm from an incident, including exfiltration of information; or	[Identical to NCPAA]
- any other cybersecurity risk attribute that cannot be used to identify specific persons believed to be unrelated to the risk, and disclosure of which is not prohibited by law	- any other cybersecurity threat attribute the disclosure of which is not prohibited by law.
- any combination of the above.	
Cybersecurity Purpose: Protecting an information system or its contents from a cybersecurity risk or incident or identifying a risk or incident source.	*Cybersecurity Purpose:* Protecting (including by using defensive measures) an information system or its contents from a cybersecurity threat or security vulnerability or identifying a threat source.
Defensive Measure: An "action, device, procedure, signature, technique, or other measure" applied to an information system that "detects, prevents or mitigates a known or suspected cybersecurity risk or incident" or attributes that could help defeat security controls, but not including measures that destroy, render unusable, or substantially harm an information system not operated by that entity or by another entity that consented to such actions.	*Defensive Measure:* An "action, device, procedure, technique, or other measure" executed on an information system or its contents that "prevents or mitigates a known or suspected cybersecurity threat or security vulnerability."
	Federal Entity: A U.S. department or agency, or any component thereof.
	Information System: As in 44 U.S.C. 3502.
	Local Government: A political subdivision of a state.
	Malicious Cyber Command and Control: "A method for unauthorized remote identification of, access to, or use of an information system" or its contents.
	Malicious Reconnaissance: A method, associated with a known or suspected cybersecurity threat, for probing or monitoring an information system to discern its vulnerabilities.
Network Awareness: Scanning, identifying, acquiring, monitoring, logging, or analyzing the contents of an information system.	*Monitor:* Scanning, identifying, acquiring, or otherwise possessing the contents of an information system.
	Non-Federal Entity: A private or governmental entity that is not federal, but not including foreign powers as defined in 50 U.S.C. 1801.

NCPAA—Title II	PCNA—Title I
Private Entity: A nonfederal entity that is an individual, nonfederal government utility or "an entity performing utility services," or	*Private Entity:* A person, nonfederal government utility, or
private group, organization, proprietorship, partnership, trust, cooperative, corporation, or other commercial or nonprofit entity, including personnel.	[Identical to NCPAA] including personnel, but not including a foreign power as defined in 50 U.S.C. 1801.
	Real Time: Automated, machine-to-machine system processing of cyber threat indicators where the occurrence and "reporting or recording" of an event are "as simultaneous as technologically and operationally practicable."
Security Control: The management, operational, and technical controls used to protect an information system and its contents against unauthorized attempts to adversely affect their confidentiality, integrity, or availability.	*Security Control:* The management, operational, and technical controls used to protect an information system and its contents against unauthorized attempts to adversely impact their confidentiality, integrity, or availability.
	Security Vulnerability: "Any attribute of hardware, software, process, or procedure that could enable or facilitate the defeat of a security control."
Sharing: "Providing, receiving, and disseminating."	
	Tribal: As in 25 U.S.C. 450b.
(b) Amendment	
Specifies tribal governments, private entities, and ISACs as appropriate members of the NCCIC in DHS.	
Sec. 203. Information Sharing Structure and Processes	**Sec. 102. Sharing of Cyber Threat Indicators and Defensive Measures by the Federal Government With Non-federal Entities**
	(a) In General
Amends Sec. 226 of the HSA.	Amends Title I of the National Security Act of 1947 by adding a new section.
	'Sec. 111. Sharing of Cyber Threat Indicators and Defensive Measures by the Federal Government With Non-Federal Entities'
	'(a) Sharing by the Federal Government'
(1) revises the functions of the NCCIC by specifying that it is the "lead" federal civilian interface for information sharing, adding "cyber threat indicators" and "defensive measures" to the subjects it addresses, and expanding its functions to include	**'(1)'** requires the DNI, in consultation with the heads of other appropriate federal entities, to develop and promulgate procedures consistent with protection of classified information, intelligence sources and methods, and privacy and civil liberties, for
- providing information and recommendations on information sharing,	
- in consultation with other appropriate agencies, collaborating with international partners, including on enhancing "the security and resilience of the global cybersecurity ecosystem," and	
- sharing "cyber threat indicators, defensive measures," and information on cybersecurity risks and incidents with federal and nonfederal entities, including across critical-infrastructure	timely sharing of classified cyber threat indicators and declassified indicators and information with relevant nonfederal entities, and sharing of information about

NCPAA—Title II	PCNA—Title I
(CI) sectors and with fusion centers. [*Note:* See also the provisions on the CTIIC in the PCNA, p. 13.]	imminent or ongoing cybersecurity threats to such entities to prevent and mitigate adverse impacts.
- notify the Secretary, the HSC, and the HSGAC of significant violations of privacy and civil liberties protections under 'Sec. 226(i)(6),'	
- promptly notifying nonfederal entities that have shared information known to be in error or in contravention to section requirements,	**'(2)'** 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.
- participating in DHS-run exercises, and	
	Requires that the procedures incorporate existing information-sharing mechanisms of federal and nonfederal entities, including ISACs, as much as possible, and
	include methods to promote efficient granting of security clearances to appropriate representatives of nonfederal entities.
(2) expands NCCIC membership to include the following [*Note:* all are existing entities]:	
- an entity that collaborates with state and local governments on risks and incidents and has a voluntary information sharing relationship with the NCCIC,	
- the US-CERT for collaboratively addressing, responding to, providing technical assistance upon request on, and coordinating information about and timely sharing of threat indicators, defensive measures, analysis, or information about cybersecurity risks and incidents,	
- the ICS-CERT to coordinate with ICS owners and operators, provide training on ICS cybersecurity, timely share information about indicators, defensive measures, or cybersecurity risks and incidents of ICS, and remain current on ICS technology advances and best practices,	
- the "National Coordinating Center for Communications to coordinate the protection, response, and recovery of emergency communications," and	
- "an entity that coordinates with small and medium-sized businesses."	
(3) adds "cyber threat indicators" and "defensive measures" to the subjects covered in the principles of operation of the NCCIC,	
	Sec. 103. Authorizations for Preventing, Detecting, Analyzing, and Mitigating Cybersecurity Threats **(f) Small Business Participation**
Requires that information be shared as appropriate with small and medium-sized businesses and that the NCCIC make self-assessment tools available to them,	Requires the Small Business Administration to assist small businesses and financial institutions in monitoring, defensive measures, and sharing information under the section. Requires a report with recommendations by the administrator to the President within one year of enactment on sharing by those institutions and use of shared information

NCPAA—Title II	PCNA—Title I
	for network defense. Requires federal outreach to those institutions to encourage them to exercise the authorities provided under the section.
Specifies that information be guarded against disclosure. Stipulates that the NCCIC must work with the DHS CPO to ensure that the NCCIC follows privacy and 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. 13.]
'(2)' requires the U/S-CIP to report to Congress twice per year on the status and progress of that capability until it is fully implemented.	
'(h) Sector Specific Agencies'	
Requires the Secretary to collaborate with relevant CI sectors and heads of appropriate federal agencies to recognize each CI SSA designated as of March 25, 2015, in the DHS National Infrastructure Protection Plan. Designates the Secretary as SSA head for each sector for which DHS is the SSA. Requires the Secretary to coordinate with relevant SSAs to - support CI sector security and resilience activities, - provide knowledge, expertise, and assistance on request, and - support timely sharing of threat indicators and defensive measures with the NCCIC.	
	[*Note:* For other provisions of 'Sec. 111(a)(2)', see pp. 11 and 20.]
	'(b) Definitions'
	Defines the following terms by reference to Sec. 110 of the title: *Appropriate Federal Entities, Cyber Threat Indicator, Defensive Measure, Federal Entity,* and *Non-Federal Entity.*
	(b) Submittal to Congress
	Requires that the procedures developed by the DNI be submitted to Congress within 90 days of enactment of the title.
	(c) Table of Contents Amendment
	Revises the table of contents of the National Security Act of 1947 to reflect the addition of 'Sec. 111'.
	Sec. 104. Sharing of Cyber Threat Indicators and Defensive Measures With Appropriate Federal Entities Other Than the Department of Defense or the National Security Agency

NCPAA—Title II	PCNA—Title I
	(a) Requirement for Policies and Procedures **(1)** Adds new subsections to 'Sec. 111' of the National Security Act of 1947
'(i) Voluntary Information Sharing Procedures'	**'(b) Policies and Procedures for Sharing with the Appropriate Federal Entities Other Than the Department of Defense or the National Security Agency'**
'(1)' permits voluntary information-sharing relationships for cybersecurity purposes between the NCCIC and nonfederal entities but prohibits requiring such an agreement. Permits the NCCIC, at the sole and unreviewable discretion of the Secretary, acting through the U/S-CIP, to terminate an agreement for repeated, intentional violation of the terms of '(i).' Permits the Secretary, solely and unreviewably and acting through the U/S-CIP, to deny an agreement for national security reasons.	**'(1)'** requires the President to develop and submit to Congress policies and procedures for federal receipt of cyber threat indicators and defensive measures.
'(2)' permits the relationship to be established through a standard agreement for nonfederal entities not requiring specific terms. 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. Stipulates that any agreement in effect prior to enactment of the title will be deemed in compliance with requirements in '(i).' Requires that those agreements include "relevant privacy protections as in effect" under the CRADA for Cybersecurity Information Sharing and Collaboration, as of December 31st 2014." Also stipulates that an agreement is not required for an entity to be in compliance with '(i).'	
	'(2)' requires that they be developed in accordance with the privacy and civil liberties guidelines under Sec. 104(b) of the title, ensure - real-time sharing of indicators from nonfederal entities with appropriate federal entities except DOD, - receipt without delay except for good cause, and - provision to all relevant federal entities, - audit capability, and - appropriate sanctions for federal personnel who knowingly and willfully use shared information other than in accordance with the title. **(2)** requires that an interim version of the policies and procedures be submitted to Congress within 90 days of enactment of the title, and the final version within 180 days. **(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'**

NCPAA—Title II	PCNA—Title I
	'(a) Establishment' 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' Permits nonfederal entities to share, for cybersecurity purposes, cyber threat indicators, and defensive measures, from their own information systems or those of other entities upon written consent, with other nonfederal entities or the NCCIC,	**Sec. 103(c) Authorization for Sharing or Receiving Cyber Threat Indicators or Defensive Measures** **(1)** permits nonfederal entities to share, for cybersecurity purposes and consistent with privacy requirements under (d)(2), lawfully obtained cyber threat indicators or defensive measures with other nonfederal entities or appropriate federal entities except DOD,
notwithstanding any other provision of law, except that recipients must comply with lawful restrictions on sharing and use imposed by the source.	[Similar to NCPAA].
	(d) Protection and Use of Information
Requires reasonable efforts by nonfederal and federal entities, prior to sharing, to safeguard personally identifying information from unintended disclosure or unauthorized access or acquisition and remove or exclude such information where it is reasonably believed when it is shared to be unrelated to a cybersecurity risk or incident.	**(2)** requires reasonable efforts by nonfederal entities, before sharing a threat indicator, to remove information reasonably believed to be personal or personally identifying of a specific person not directly related to a cybersecurity threat, or implement a technical capability for removing such information.
	Sec. 109. Construction and Preemption **(f) Information Sharing Relationships**
Stipulates that nothing in '(3)'	Stipulates that nothing in the title

NCPAA—Title II	PCNA—Title I
- limits or modifies an existing information sharing relationship or prohibits or requires a new one,	- **(1)** limits or modifies an existing information sharing relationship or **(2)** prohibits or requires a new one,
	Sec. 103(c)(3) stipulates that nothing in (c) - authorizes information sharing other than as provided in (c), - permits unauthorized sharing of classified information, - authorizes federal surveillance of any person, - prohibits a federal entity, at the request of a nonfederal entity, from technical discussion of threat indicators and defensive measures and assistance with vulnerabilities and threat mitigation, - prohibits otherwise lawful sharing by a nonfederal entity of indicators or defensive measures with DOD, or
- limits otherwise lawful activity, or - impacts or modifies existing procedures for reporting criminal activity to appropriate law enforcement authorities, or participating in an investigation.	- limits otherwise lawful activity.
Requires the U/S-CIP to coordinate with stakeholders to develop and implement policies and procedures to coordinate disclosures of vulnerabilities as practicable and consistent with relevant international industry standards.	
'(4) Network Awareness Authorization'	**(a) Authorization for Private-Sector Defensive Monitoring**
permits nonfederal, nongovernment entities, notwithstanding any other provision of law, to conduct network awareness, for cybersecurity purposes and to protect rights or property, of	**(1)** permits private entities, notwithstanding any other provision of law, to monitor, for cybersecurity purposes,
- its own information systems,	[Similar to NCPAA],
- with written consent, information systems of a nonfederal or federal entity, or	[Similar to NCPAA], or
- the contents of such systems.	[Similar to NCPAA].
Stipulates that nothing in '(4)' - authorizes network awareness other than as provided in the section, or - limits otherwise lawful activity,	**(2)** Stipulates that nothing in (a) - authorizes monitoring other than as provided in the title, - limits otherwise lawful activity, or - authorizes federal surveillance of any person.
'(5) Defensive Measure Authorization'	**(b) Authorization for Operation of Defensive Measures**
permits nonfederal, nongovernment entities to operate defensive measures, for cybersecurity purposes and to protect rights or property, that are applied to	**(1)** permits private entities to operate defensive measures, for cybersecurity purposes and to protect rights or property, that are operated on
- its own information systems,	[Similar to NCPAA], or
- with written consent, information systems of a nonfederal or federal entity, or	[Similar to NCPAA],
- the contents of such systems,	
notwithstanding any other provision of law, except that measures may not be used except as authorized in the section, and '(5)' does not limit otherwise lawful activity.	**(3)** notwithstanding any other provision of law, except that measures may not be used except as authorized in (b), and (b) does not limit otherwise lawful activity.
	(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

NCPAA—Title II	PCNA—Title I
	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.
	(e) No Right or Benefit
	Stipulates that sharing of indicators with a nonfederal entity creates no right or benefit to similar information by any nonfederal entity.
'(6) Privacy and Civil Liberties Protections'	**Sec. 104(b) Privacy and Civil Liberties**
Requires the U/S-CIP, in coordination with the DHS CPO and Chief Civil Rights and Civil Liberties Officer,	**(1)** requires the AG, in consultation with appropriate federal agency heads and agency privacy and civil liberties officers,
to establish and review annually policies and procedures on information shared with the NCCIC under the section.	to develop and review periodically guidelines on privacy and civil liberties to govern federal handling of cyber threat indicators obtained through the title's provisions.
Requires that they apply only to DHS, consistent with the need for timely protection of information systems from and mitigation of cybersecurity risks and incidents, the policies and procedures	**(2)** requires that, consistent with the need for protection of information systems and threat mitigation, the guidelines
- be consistent with DHS Fair Information Practice Principles,	- be consistent with Fair Information Practice Principles 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"],
- "reasonably limit, to the extent practicable, receipt, retention, use, and disclosure of cybersecurity threat indicators and defensive measures associated with specific persons" not needed for timely protection of systems and networks,	- limit receipt, retention, use, and dissemination of cybersecurity threat indicators containing personal information of or identifying specific persons,
	including by establishing processes for prompt destruction of information known not to be directly related to uses under the title, and notification of recipients that indicators may be used only for cybersecurity purposes, and setting limitations on retention of indicators,
- minimize impacts on privacy and civil liberties,	- limit impacts on privacy and civil liberties of federal activities under the title, including
- provide data integrity through prompt removal and destruction of obsolete or erroneous personal information unrelated to the information shared and retained by the NCCIC in accordance with this section,	guidelines for removal of personal and personally identifying information handled by federal entities under the title,
- include requirements to safeguard from unauthorized access or acquisition cyber threat indicators and defensive measures retained by the NCCIC, identifying specific persons, including proprietary or business-sensitive information,	- include requirements to safeguard from unauthorized access or acquisition cyber threat indicators containing personal information of or identifying specific persons,
- protect the confidentiality of cyber threat indicators and defensive measures associated with specific persons, to the greatest extent practicable,	
- ensure that relevant constitutional, legal, and privacy protections are observed.	- be consistent with other applicable provisions of law,
	- include procedures to notify entities if a federal entity receiving information knows that it is not a cyber threat

NCPAA—Title II	PCNA—Title I
	indicator, - include steps to ensure that dissemination of indicators is consistent with the protection of classified and other sensitive national security information.
Stipulates that the U/S-CIP may consult with NIST in developing the policies and procedures.	
Requires the DHS CPO and the Officer for Civil Rights and Civil Liberties, in consultation with the PCLOB, to submit to appropriate congressional committees the policies and procedures within 180 days of enactment and annually thereafter.	Requires the AG to submit to Congress interim guidelines within 90 days of enactment and final guidelines within 180 days.
Requires the U/S-CIP, in consultation with the PCLOB and the DHS CPO and Chief Civil Rights and Civil Liberties Officer, to ensure public notice of and access to the policies and procedures.	
Requires the DHS CPO to - monitor implementation of the policies and procedures, - submit to Congress an annual review on their effectiveness, - work with the U/S-CIP to carry out provisions in '(c)' on notification about violations of privacy and civil liberties policies and procedures and about information that is erroneous or in contravention of section requirements, - regularly review and update impact assessments as appropriate to ensure that all relevant protections are followed, and	
- ensure appropriate sanctions for DHS personnel who knowingly and willfully conduct unauthorized activities under the section.	**Sec. 104(b)(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.],
	Sec. 107. Oversight of Government Activities **(b) Reports on Privacy and Civil Liberties.**
Requires the DHS IG, in consultation with the PCLOB and IGs of other agencies receiving shared indicators or defensive measures from the NCCIC, to submit a report to HSC and HSGAC within two years of enactment and periodically thereafter reviewing such information, including	**(2)** requires the IGs of DHS, the IC, DOJ, and DOD to jointly submit a biennial report to Congress on
- receipt, use, and dissemination of cybersecurity indicators and defensive measures shared with federal entities under the section,	- receipt, use, and dissemination of cybersecurity indicators and defensive measures shared with federal entities under the title,
- information on NCCIC use of such information for purposes other than cybersecurity,	
- types of information shared with the NCCIC,	- types of indicators shared with federal entities,
- actions taken by NCCIC based on shared information;	- actions taken by federal entities as a result of receiving shared indicators,
- metrics to determine impacts of sharing on privacy and civil liberties,	
- a list of federal agencies receiving the information,	- a list of federal entities receiving the indicators,
- identification of inappropriate stovepiping of shared	- identification of inappropriate barriers to sharing

NCPAA—Title II	PCNA—Title I
information, and	information,
	- procedures for sharing information and removal of personal and identifying information, and incidents involving improper treatment of it, and
- recommendations for improvements or modifications to sharing under the section.	- recommendations for improvements or modifications to authorities under the title.
	Requires that the reports be submitted in unclassified form but permits a classified annex.
	Requires public availability of unclassified parts of the reports.
Requires the DHS CPO and Chief Civil Rights and Civil Liberties Officer, in consultation with the PCLOB, the DHS IG, and senior privacy and civil liberties officers of each federal agency receiving indicators or defensive measures shared with the NCCIC, to	**(1)** requires the PCLOB to
submit a biennial report to Congress	submit a biennial report to Congress and the President
assessing impacts on privacy and civil liberties of federal activities under '(6)', including	assessing impacts of activities under the title on and sufficiency of policies, procedures, and guidelines in addressing concerns about privacy and civil liberties, including
recommendations to minimize or mitigate such impacts.	recommendations for improvements or modifications to authorities under the title.
	Requires that the reports be submitted in unclassified form but permits a classified annex.
	Requires public availability of unclassified parts of the reports.
	(a) Biennial Report on Implementation
	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, including
	- review of types of indicators shared with the federal government,
	- 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,
	- assessment of sufficiency of policies, procedures, and guidelines to ensure effective and responsible sharing under Sec. 4 [sic] of the PCNA,
	- sufficiency of procedures under Sec. 3 [sic] for timely sharing,
	- appropriateness of classification of indicators and accounting of security clearances authorized,
	- federal actions taken based on shared indicators, including appropriateness of subsequent use or dissemination under the title,
	- description of any significant federal violations of the requirements of the title, including assessments of all reports

NCPAA—Title II	PCNA—Title I
	of federal personnel misusing information provided under the title and all disciplinary actions taken, and - 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. **'(3)'** permits reports to include recommendations for improvements or modifications to authorities and processes under the title. **'(4)'** requires that the reports be submitted in unclassified form but permits a classified annex. **'(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** **(d) Protection and Use of Information**
[Nonfederal Entities]	
Permits a nonfederal, nongovernment entity that shares indicators or defensive measures with the NCCIC to	**(3)** permits a nonfederal entity [*Note:* including government entities], for a cybersecurity purpose, to
use, retain, or disclose indicators and defensive measures, solely for cybersecurity purposes.	use indicators or defensive measure shared or received under (d) to monitor or operate a defensive measure on its own information systems or those of other nonfederal or federal entities upon written authorization from them, with
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. 14, 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.
Stipulates that the information shall be deemed voluntarily shared.	
Requires implementation and utilization of security controls to protect against unauthorized access or acquisition.	**(1)** requires implementation of appropriate security controls to protect against unauthorized access or acquisition.
Prohibits use of such information to gain an unfair competitive advantage.	
[Federal Entities]	**Sec. 104(d) Information Shared with or Provided to the Federal Government**
Permits federal entities receiving indicators or defensive measures from the NCCIC or otherwise under the section to use, retain, or further disclose it solely for	**(5)** permits federal entities or personnel receiving indicators or defensive measures under the title to, consistent with otherwise applicable provisions of federal law, use, retain, or disclose it solely for
cybersecurity purposes.	a cybersecurity purpose,
[*Note:* Sec. 216 (see p. 29) permits use of information obtained from federal systems for investigating, prosecuting,	responding to, investigating, prosecuting, or otherwise

NCPAA—Title II	PCNA—Title I
disrupting, or otherwise responding to	preventing or mitigating
imminent threats of death or serious bodily harm	threats of death or serious bodily harm or offenses arising out of such threats,
serious threats to minors, including sexual exploitation or threats to physical safety, and	serious threats to minors, including sexual exploitation and threats to physical safety, and
violations of 18 U.S.C. 1030 [computer fraud], or	- preventing, investigating, disrupting, or prosecuting offenses listed in 18 U.S.C. 1028-30, 3559(c)(2)(F), and Ch. 37 and 90 [computer fraud and identity theft, espionage and censorship, protection of trade secrets, and serious violent felonies].
attempts or conspiracy to commit the above offenses.]	
	Prohibits federal disclosure, retention, or use for any purpose not permitted under (5).
Requires reasonable efforts prior to sharing to safeguard personally identifying information from unintended disclosure and unauthorized access or acquisition, and remove or exclude such information where it is reasonably believed when shared to be unrelated to a cybersecurity risk or incident.	Stipulates that the policies, procedures, and guidelines in (a) [on provision of information to the federal government] and (b) [on privacy and civil liberties] of the title apply to such information. **'Sec. 111(a)(2)'** requires that procedures for sharing developed by the DNI 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 do so.
Stipulates that the indicators and defensive measures shall be deemed voluntarily shared.	**Sec. 104(d)(3)** stipulates that the information shall be deemed voluntarily shared.
Requires implementation and utilization of security controls to protect against unauthorized access or acquisition.	**'Sec. 111(a)(2)'** requires that procedures for sharing developed by the DNI include requirements for federal entities to implement security controls to protect against unauthorized access to or acquisition of shared information.
	Sec. 109(a) Prohibition of Surveillance
Prohibits use in surveillance or collection activities to track an individual's personally identifiable information except as authorized in the section.	Stipulates that the title does not authorize DOD or any element of the IC to target a person for surveillance.
Stipulates that the 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)** [Similar to NCPAA], and
	exempt from disclosure under nonfederal disclosure laws, except for those requiring disclosure in criminal prosecutions.
Prohibits use for regulatory purposes.	[*Note:* No specific corresponding prohibition, but Sec. 104(d)(5) above prohibits federal disclosure, retention, or use for any purpose other than those specified in the paragraph.]
Specifies that there is no waiver of applicable privilege or protection under law, including trade-secret protection;	**(1)** [Similar to NCPAA].
Requires that the information be considered the commercial, financial, and proprietary information of the nonfederal entity when so designated by it.	**(2)** requires that, consistent with Sec. 103(c)(2), the information be considered the commercial, financial, and proprietary information of the originating nonfederal source, when so designated by such source or nonfederal entity acting with written authorization from it.
Stipulates that the information is not subject to judicial	**(4)** [Similar to NCPAA]

NCPAA—Title II	PCNA—Title I
doctrine or rules of federal entities on ex-parte communications.	
[Nonfederal Government Entities]	[*Note:* See also Nonfederal Entities, p. 19]
Permits state, local, and tribal government to	**Sec. 103(d)(4)** permits state, local, and tribal government entities
use, retain, or further disclose indicators or defensive measures shared under the section solely for cybersecurity purposes.	to use shared cyber threat indicators for cybersecurity purposes,
	responding to, prosecuting, or otherwise preventing or mitigating threats of death or serious bodily harm or offenses arising out of such threats, or responding to serious threats to minors, 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. 14, describing requirements for removal of personal information].
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. 19.]
Stipulates that the indicators and defensive measures shall be deemed voluntarily shared.	Stipulates that such shared indicators or defensive measures be deemed voluntarily shared and exempt from disclosure, and
Requires implementation and utilization of security controls to protect against unauthorized access or acquisition.	
Exempts the information from disclosure under nonfederal disclosure laws or regulations.	exempts the shared indicators from disclosure under nonfederal disclosure laws or regulations, except as required in criminal prosecutions.
Prohibits use for regulation of lawful activities of nonfederal entities.	
'(8) Liability Exemptions'	**Sec. 106. Protection from Liability**
	(a) Monitoring of Information Systems
States that "no cause of action shall lie or be maintained in any court" against nonfederal, nongovernment entities for conducting network awareness under '(4)' in accordance with the section or	States that "no cause of action shall lie or be maintained in any court" against private entities for monitoring information systems under Sec. 103(a) conducted in accordance with the title or
	(b) Sharing or Receipt of Cyber Threat Indicators
for sharing indicators or defensive measures under '(3),' or a good-faith failure to act if sharing is done in accordance with the section.	for information sharing under Sec. 103(c) in accordance with the title or a failure to act if sharing is done in accordance with the title.
Stipulates that nothing in the section	**(c)(1)** stipulates that nothing in the section
- requires dismissal of a cause of action against a nonfederal, nongovernment entity that engages in willful misconduct in the course of activities under the section.	- requires dismissal of a cause of action against a nonfederal entity that engages in willful misconduct in the course of activities under the title, or
- undermines or limits availability of otherwise applicable	[Identical to NCPAA]

NCPAA—Title II	PCNA—Title I
common law or statutory defenses.	
Establishes the burden of proof as clear and convincing evidence from the plaintiff of injury-causing gross negligence or willful misconduct,	**(2)** [Similar to NCPAA]
Defines *willful misconduct* as an act or omission taken intentionally to achieve a wrongful purpose, knowingly without justification, and in disregard of risk of highly probable harm that outweighs any benefit.	**(3)** [Similar to NCPAA].
'(9) Federal Government Liability for Violations of Restrictions on the Use and Protection of Voluntarily Shared Information'	**Sec. 105. Federal Government Liability for Violations of Privacy or Civil Liberties**
	(a) In General
Makes the federal government liable to injured persons for intentional or willful violation of restrictions on federal disclosure and use under 'Sec. 226', with minimum damages of $1,000 plus	Makes the federal government liable to injured persons for intentional or willful violation of privacy and civil liberties guidelines under Sec. 104(b), with minimum damages of $1,000 plus
reasonable attorney fees as determined by the court and other reasonable litigation costs in any case under (a) where "the complainant has substantially prevailed."	[Identical to NCPAA]
	(b) Venue
Stipulates the federal district courts where the case may be brought as the one in which the complainant resides or the principal place of business is located, the District of Columbia, or	[Identical to NCPAA]
where the federal department or agency that disclosed the information is located.	where the federal department or agency that violated the guidelines is located.
	(c) Statute of Limitations
Sets the statute of limitations under '(i)' at two years from the date on which the cause of action arises.	Sets the statute of limitations under Sec. 105 at two years from the date on which the cause of action arises.
	(d) Exclusive Cause of Action.
Sets action under '(i)' as the exclusive remedy for violation of restrictions under '(i)(3),' '(i)(6),' or '(i)(7)(B)'.	Sets action under (d) as the exclusive remedy for federal violations under the title.
'(10) Anti-Trust Exemption'	
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.	
'(11) Construction and Preemption'	**Sec. 109(b) Otherwise Lawful Disclosures**
Stipulates that the section does not limit or prohibit otherwise lawful disclosures or participation in an investigation by a nonfederal entity of information to any other federal or nonfederal entity.	Stipulates that the title 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, whether or not the disclosures duplicate those made under the title.
	(c) Whistle Blower Protections
Stipulates that the section 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, 50 U.S.C. 3234, or similar provisions of	Stipulates that the title does not prohibit or limit disclosures protected under 5 U.S.C. 2302(b)(8), 5 U.S.C. 7211, 10

NCPAA—Title II	PCNA—Title I
federal or state law.	U.S.C. 1034, or similar provisions of federal or state law.
	(e) Relationship to Other Laws
Stipulates that the section does not affect any requirements under other provisions of law for nonfederal entities providing information to federal entities.	Stipulates that the title does not affect any requirements under other provisions of law for nonfederal entities providing information to federal entities.
	(g) Preservation of Contractual Obligations and Rights
Stipulates that the section does not change contractual relationships between nonfederal entities or them and federal entities or abrogate trade-secret or intellectual property rights.	Stipulates that the title does not change contractual relationships between nonfederal entities or them and federal entities, or abrogate trade-secret or intellectual property rights.
	(h) Anti-Tasking Restriction
Stipulates that the section does not permit the federal government to require nonfederal entities to provide it with information, or condition sharing of indicators or defensive measures on provision by such entities of indicators or defensive measures, or condition award of grants, contracts, or purchases on such provision.	Stipulates that the title does not permit the federal government to require nonfederal entities to provide it with information, or condition sharing of indicators on provision of indicators, or condition award of grants, contracts, or purchases on such provision.
	(i) No Liability for Non-Participation
Stipulates that the section does not create liabilities for any nonfederal entities that choose not to engage in the voluntary activities authorized in the section.	Stipulates that the title does not create liabilities for any nonfederal entities that choose not to engage in the voluntary activities authorized in the title.
	(j) Use and Retention of Information
Stipulates that the section 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 section. Stipulates that the section does not restrict or condition sharing for cybersecurity purposes among nonfederal entities or require sharing by them with the NCCIC. Prohibits specified monopolistic activities such as price-fixing.	Stipulates that the title 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 title.
	(k) Federal Preemption
Specifies that the section supersedes state and local laws relating to its provisions	**(1)** specifies that the title supersedes state and local laws relating to its provisions. **(2)** stipulates that the title does not supersede state and local laws on use of authorized law enforcement practices and procedures. **(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	

NCPAA—Title II	PCNA—Title I
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 the President or federal entities to protect and control dissemination of classified information, sources and methods, and U.S. national security.
Sec. 204. Information Sharing and Analysis Organizations Amends Sec. 212 of the HSA to **(1)** broaden the functions of ISAOs to include cybersecurity risk and incident information beyond that relating to critical infrastructure, and **(2)** add by reference the definitions of *cybersecurity risk* and *incident* in 6 U.S.C. 148(a).	
Sec. 205. Streamlining of Department of Homeland Security Cybersecurity and Infrastructure Protection Organization **(a) Cybersecurity and Infrastructure Protection Directorate** Renames the DHS National Protection and Programs Directorate as the Cybersecurity and Infrastructure Protection. [*Sic.*]	
(b) Senior Leadership of the Cybersecurity and Infrastructure Protection Directorate Provides a specific title for the undersecretary in charge of critical infrastructure protection as U/S-CIP. Also adds two deputy undersecretaries, one for cybersecurity and the other for infrastructure protection. Does not require new appointments for current officeholders and specifies that appointment of the undersecretaries does not require Senate confirmation.	
(c) Report Requires a report to HSC and HSGAC from the U/S-CIP within 90 days of enactment on the feasibility of becoming an operational component of DHS, If that is determined to be the best option for mission fulfillment, requires submission of a legislative proposal and implementation plan. Also requires that the report include plans for more effective execution of the cybersecurity mission, including expediting of information sharing agreements.	

NCPAA—Title II	PCNA—Title I
Sec. 206. Cyber Incident Response Plans **(a) In General** Amends Sec. 227 of the HSA to change "Plan" to "Plans" in the title, to specify the U/S-CIP as the responsible official, and to add a new subsection: **'(b) Updates to the Cyber Incident Annex to the National Response Framework'** Requires the Secretary, in coordination with other agency heads and in accordance with the National Cybersecurity Incident Response Plan, to update, maintain, and exercise regularly the Cyber Incident Annex to the DHS National Response Framework. **(b) Clerical Amendment** Amends the table of contents of the act to reflect the title change made by (a). **Sec. 207. Security and Resiliency of Public Safety Communications; Cybersecurity Awareness Campaign** **(a) In General** Adds two new sections to the HSA: **'Sec. 230. Security and Resiliency of Public Safety Communications'** 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. **'Sec. 231. Cybersecurity Awareness Campaign'** **'(a) In General'** Requires the U/S-CIP to develop and implement an awareness campaign on risks and best practices for mitigation and response, including at a minimum public service announcements and information on best practices that are vendor- and technology-neutral. **'(b) Consultation'** Requires consultation with a wide range of stakeholders. **'Sec. 232. National Cybersecurity Preparedness Consortium'** **'(a) In General'** Authorizes the Secretary to establish the National Cybersecurity Preparedness Consortium to **'(b) Functions'** - provide cybersecurity training to state and local first responders and officials, - establish a training curriculum for them using the DHS Community Cyber Security Maturity Model,	

NCPAA—Title II	PCNA—Title I
- provide technical assistance for improving capabilities, - conduct training and simulation exercises, - coordinate with the NCCIC to help states and communities develop information sharing programs, and - coordinate with the National Domestic Preparedness Consortium to incorporate cybersecurity into emergency management functions. **'(c) Members'** Stipulates that members be academic, nonprofit, and government partners with prior experience conducting cybersecurity training and exercises in support of homeland security. **(b) Clerical Amendment** Amends the table of contents of the act to include the new sections. **Sec. 208. Critical Infrastructure Protection Research and Development** **(a) Strategic Plan; Public-Private Consortiums** Adds a new section to the HSA: **'Sec. 318. Research and Development Strategy for Critical Infrastructure Protection'** **'(a) In General'** Requires the Secretary to submit to Congress within 180 days of enactment, and biennially thereafter, a strategic plan to guide federal R&D in technology relating to both cyber- and physical security for CI. **'(b) Contents of Plan'** Requires the plan to include - CI risks and technology gaps identified in consultation with stakeholders and a resulting risk and gap analysis, - prioritized needs based on that analysis, emphasizing technologies to address rapidly evolving threats and technology and including clearly defined roadmaps, - facilities and capabilities required to meet those needs, - current and planned programmatic initiatives to foster technology advancement and deployment, including collaborative opportunities, and - progress on meeting plan requirements. **'(c) Coordination'** Requires coordination between the DHS Under Secretaries for Science and Technology and for the National Protection and Programs Directorate. [*Note:* Sec. 205 renames the latter position as the U/S-CIP.] **'(d) Consultation'** Requires the Under Secretary for Science and Technology to consult with CI Sector Coordinating Councils, heads of other relevant federal agencies, and state, local, and tribal governments as appropriate. **(b) Clerical Amendment**	

NCPAA—Title II	PCNA—Title I
Amends the table of contents of the act to include the new section.	
Sec. 209. Report on Reducing Cybersecurity Risks in DHS Data Centers Requires a report to HSC and HSGAC within one year of enactment on the feasibility of creating an environment within DHS for reduction in cybersecurity risks in data centers, including but not limited to increased compartmentalization of systems with a mix of security controls among compartments.	
	Sec. 108. Report on Cybersecurity Threats **(a) Report Required** Requires the DNI, in consultation with heads of other appropriate elements of the IC, to submit within 180 days of enactment a report to the House and Senate Intelligence Committees on cybersecurity threats to the U.S. national security and economy, including attacks, theft, and data breaches. **(b) Contents** 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, **(2)** a list and assessment of countries and nonstate actors constituting the primary sources of such threats, **(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, **(4)** assessment of additional technologies or capabilities that would enhance the U.S. ability to prevent and respond to such threats, and **(5)** assessment of private-sector technologies or practices that could be rapidly fielded to assist the IC in preventing and responding to such threats. **(c) Form of Report** Requires that the report be unclassified, but may include a classified annex. **(d) Public Availability of Report** Requires that the unclassified portion of the report be publicly available. **(e) Intelligence Community Defined** Defines intelligence community as in 50 U.S.C. 3003.
Sec. 210. Assessment Requires the Comptroller General, within two years of	

NCPAA—Title II	PCNA—Title I
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 Stipulates that the title does not grant DHS new authority to promulgate regulations or set standards relating to cybersecurity for nonfederal, nongovernmental entities.	**Sec. 109(l) Regulatory Authority** 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.
Sec. 214 Sunset Ends all requirements for reports in the title seven years after enactment.	
Sec. 215. Prohibition on New Funding Stipulates that the title does not authorize additional funds for implementation and must be carried out using available amounts.	
Sec. 216. Protection of Federal Information Systems **(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,	

NCPAA—Title II	PCNA—Title I
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. 19).]
'(c) Conditions' 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 Terminates the provisions in the title seven years after enactment.	**Sec. 112 Sunset** [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 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 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.	**Sec. 111. Comptroller General Report on Removal of Personal Identifying Information** **(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).

NCPAA—Title II	PCNA—Title I
	(b) Form Requires that the report be unclassified but permits a classified annex.

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

Acknowledgments

Stephanie Logan, an intern, provided valuable assistance with the comparative analysis and other preparation for this report.