



**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

**Stephanie M. Logan**

Research Assistant

June 4, 2015

**Congressional Research Service**

7-5700

[www.crs.gov](http://www.crs.gov)

R43996

## 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 114<sup>th</sup> 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**

House Consideration of the Two Bills .....	1
Current Legislative Proposals .....	2
Comparison of the NCPAA and the PCNA .....	5
Glossary of Abbreviations in the Table .....	5
Notes on the Table .....	6

## **Tables**

Table 1. Side-by-Side Comparison of the Two Titles of H.R. 1560 as Passed by the House—the PCNA (Title 1) and the NCPAA (Title II) .....	7
--	---

## **Contacts**

Author Contact Information.....	29
---------------------------------	----

This report compares provisions in two bills in the House of Representatives that address information sharing and related activities in cybersecurity:<sup>1</sup>

- H.R. 1560, the Protecting Cyber Networks Act (PCNA), as passed by the House on April 22; and
- H.R. 1731, the National Cybersecurity Protection Advancement Act of 2015 (NCPAA), as passed by the House on April 23.<sup>2</sup>

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.<sup>3</sup> 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 terminating the bill's provisions seven years after enactment, which passed by recorded vote of

---

<sup>1</sup> The analysis is limited to a textual comparison of the bills and is not intended to reach any legal conclusions regarding them.

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

<sup>3</sup> 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>.

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 114<sup>th</sup> Congress, three in the House and two in the Senate. The White House has also submitted a legislative proposal<sup>4</sup> (WHP) and issued an executive order on the topic.<sup>5</sup> Other proposals include the following:

- The Cyber Intelligence Sharing and Protection Act (CISPA), which passed the House in the 113<sup>th</sup> Congress, has been reintroduced as H.R. 234.
- S. 456 is an amended version of the White House proposal.<sup>6</sup>
- 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 113<sup>th</sup> 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.<sup>7</sup> 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

---

<sup>4</sup> 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>.

<sup>5</sup> 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>.

<sup>6</sup> 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.

<sup>7</sup> 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](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),<sup>8</sup> 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).<sup>9</sup> 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.<sup>10</sup>

On February 20, 2015, President Obama signed Executive Order 13691,<sup>11</sup> which 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 the ISAOs.<sup>12</sup> It also requires the NCCIC to coordinate with ISAOs on information sharing, and includes some provisions to facilitate sharing of classified cybersecurity information with appropriate entities.

On April 21, the White House announced support for passage of both the NCPAA and the 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.<sup>13</sup> It also called for clarifying provisions in the NCPAA on use of shared information in federal law enforcement and ensuring that provisions in the PCNA do not interfere with privacy and civil liberties protections.

---

<sup>8</sup> The IC consists of 17 agencies and others as designated under 50 U.S.C. 3003.

<sup>9</sup> 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>).

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

<sup>11</sup> Executive Order 13691, "Promoting Private Sector Cybersecurity Information Sharing."

<sup>12</sup> 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>).

<sup>13</sup> 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](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](https://www.whitehouse.gov/sites/default/files/omb/legislative/sap/114/saphr1731r_20150421.pdf).

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 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 passed by the House on May 15, 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.<sup>14</sup> 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.<sup>15</sup> In addition, most information sharing relates to imminent or near-term threats. It is not directly relevant to broader issues in

---

<sup>14</sup> 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>.

<sup>15</sup> 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>).



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.

## **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.<sup>16</sup> 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. 14, 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.

---

<sup>16</sup> This approach was taken for purposes of efficiency and convenience only. CRS does not advocate or take positions on legislation or legislative issues.

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

**Table I. 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
<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><b>Sec. 201. Short Title</b></p> <p>National Cybersecurity Protection Advancement Act of 2015</p> <p><b>Sec. 202. National Cybersecurity and Communications Integration Center</b></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><b>(a) In General</b></p> <p>Amends existing definitions:</p> <p><i>Cybersecurity Risk:</i> Excludes actions solely involving violations of consumer terms of service or licensing agreements from the definition.</p> <p><i>Incident:</i> 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.”</p> <p>Adds the following definitions:</p> <p><i>Cyber Threat Indicator:</i> <u>Technical</u> information necessary to describe or identify</p> <ul style="list-style-type: none"> <li>- 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</li> <li>- communications that <u>reasonably</u> appear to have “the</li> </ul>	<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><b>Sec. 101. Short Title</b></p> <p>Protecting Cyber Networks Act</p> <p><b>Sec. 110. Definitions</b></p> <p><i>Agency:</i> As in 44 U.S.C. 3502.</p> <p><i>Appropriate Federal Entities:</i> Departments of Commerce, Defense, Energy, Homeland Security, Justice, and the Treasury; and Office of the ODNI.</p> <p><i>Cybersecurity Threat:</i> An action unprotected by the 1<sup>st</sup> 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.</p> <p><i>Cyber Threat Indicator:</i> Information or a <u>physical object</u> necessary to describe or identify</p> <ul style="list-style-type: none"> <li>- malicious reconnaissance, including</li> <li>- <u>anomalous patterns of</u> communications that appear to have</li> </ul>

NCPAA—Title II	PCNA—Title I
<p>purpose of gathering technical information related to a cybersecurity <u>risk</u>,”</p> <ul style="list-style-type: none"><li>- a method for defeating a <u>technical or</u> security control,</li><li>- a <u>technical</u> vulnerability including anomalous <u>technical behavior</u> that may become a vulnerability,</li><li>- a method of causing a legitimate user of an information system or its contents to <u>inadvertently</u> enable defeat of a <u>technical or operational</u> control,</li><li>- 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</li><li>- actual or potential harm from an incident, including exfiltration of information; or</li><li>- any other cybersecurity <u>risk</u> 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</li><li>- any combination of the above.</li></ul> <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 that “<u>detects</u>, prevents or mitigates a known or suspected cybersecurity <u>risk or incident</u>” or attributes that could help defeat security controls, but not including measures that destroy, render unusable, or substantially harm an information system or its contents not operated by that nonfederal entity, except a state, local, or tribal government, or by another nonfederal or federal entity that consented to such actions.</p> <p><i>Network Awareness:</i> Scanning, identifying, acquiring, monitoring, logging, or <u>analyzing</u> the contents of an information system.</p>	<p>“the purpose of gathering technical information related to a cybersecurity <u>threat or security vulnerability</u>,”</p> <ul style="list-style-type: none"><li>- a method of defeating a security control or <u>exploiting a security vulnerability</u>,</li><li>- a <u>security</u> vulnerability or anomalous activity indicating the existence of one,</li><li>- 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 exploitation of a security vulnerability</u>,</li><li>- “malicious cyber command and control,”</li></ul> <p>[Identical to NCPAA]</p> <ul style="list-style-type: none"><li>- any other cybersecurity <u>threat</u> attribute the disclosure of which is not prohibited by law.</li></ul> <p>[No Corresponding Provision]</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. 15];</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><i>Local Government:</i> A political subdivision of a state.</p> <p><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.</p> <p><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.</p> <p><i>Monitor:</i> Scanning, identifying, <u>acquiring, or otherwise possessing</u> the contents of an information system.</p>

NCPAA—Title II	PCNA—Title I
<p><i>Private Entity:</i> A nonfederal entity that is an <u>individual</u>, nonfederal government utility or “an entity performing utility services,” or</p> <p>private group, organization, proprietorship, partnership, trust, cooperative, corporation, or other commercial or nonprofit entity, including personnel.</p> <p><i>Security Control:</i> The management, operational, and technical controls used to protect an information system and the information stored on, processed by, or transiting it against unauthorized attempts to adversely <u>affect</u> their confidentiality, integrity, or availability.</p> <p><i>Sharing:</i> “Providing, receiving, and disseminating.”</p> <p><b>(b) Amendment</b></p> <p>Specifies tribal governments, private entities, and ISACs as appropriate members of the NCCIC in DHS.</p> <p><b>Sec. 203. Information Sharing Structure and Processes</b></p> <p>Amends Sec. 226 of the HSA.</p> <p><b>(1)</b> 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> <ul style="list-style-type: none"> <li>- providing information and recommendations on information sharing,</li> <li>- in consultation with other appropriate agencies, collaborating with international partners, including on enhancing “the security and resilience of the global</li> </ul>	<p><i>Non-Federal Entity:</i> A private or governmental entity that is not federal, but not including foreign powers as defined in 50 U.S.C. 1801.</p> <p><i>Private Entity:</i> A <u>person</u>, nonfederal government utility, or</p> <p>[Identical to NCPAA]</p> <p>including personnel, but not including a foreign power as defined in 50 U.S.C. 1801.</p> <p><i>Real Time:</i> 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.”</p> <p><i>Security Control:</i> The management, operational, and technical controls used to protect an information system and its information against unauthorized attempts to adversely <u>impact</u> their 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><i>Tribal:</i> As in 25 U.S.C. 450b.</p> <p><b>Sec. 102. Sharing of Cyber Threat Indicators and Defensive Measures by the Federal Government With Non-federal Entities</b></p> <p><b>(a) In General</b></p> <p>Amends Title I of the National Security Act of 1947 by adding a new section.</p> <p><b>‘Sec. 111. Sharing of Cyber Threat Indicators and Defensive Measures by the Federal Government With Non-Federal Entities’</b></p> <p><b>‘(a) Sharing by the Federal Government’</b></p> <p><b>‘(1)’</b> 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>

NCPAA—Title II	PCNA—Title I
<p>cybersecurity ecosystem,” and</p> <ul style="list-style-type: none"><li>- 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. 12.]</li><li>- notify the Secretary, the HSC, and the HSGAC of significant violations of privacy and civil liberties protections under ‘Sec. 226(i)(6),’</li><li>- promptly notifying nonfederal entities that have shared information known to be in error or in contravention to section requirements,</li></ul> <p>- participating in DHS-run exercises, and</p> <p><b>(2)</b> expands NCCIC membership to include the following [Note: all are existing entities]:</p> <ul style="list-style-type: none"><li>- an entity that collaborates with state and local governments on risks and incidents and has a voluntary information sharing relationship with the NCCIC,</li><li>- 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,</li><li>- 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,</li><li>- the “National Coordinating Center for Communications to coordinate the protection, response, and recovery of emergency communications,” and</li><li>- “an entity that coordinates with small and medium-sized businesses.”</li></ul> <p><b>(3)</b> adds “cyber threat indicators” and “defensive measures” to the subjects covered in the principles of operation of the NCCIC,</p> <p>Requires that information be shared as appropriate with small and medium-sized businesses and that the NCCIC make self-</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><b>‘(2)’</b> 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>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.</p> <p><b>Sec. 103. Authorizations for Preventing, Detecting, Analyzing, and Mitigating Cybersecurity Threats</b></p> <p><b>(f) Small Business Participation</b></p> <p>Requires the Small Business Administration to assist small businesses and financial institutions in monitoring, defensive</p>

NCPAA—Title II	PCNA—Title I
<p>assessment tools available to them,</p> <p>Specifies that information be guarded against disclosure.</p> <p>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)’;</p> <p><b>(4)</b> adds new subsections to Sec. 226 of the HSA:</p> <p><b>‘(g) Rapid Automated Sharing’</b></p> <p><b>‘(1)’</b> 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)’.</p> <p><b>‘(2)’</b> 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.</p> <p><b>‘(h) Sector Specific Agencies’</b></p> <p>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</p> <ul style="list-style-type: none"><li>- support CI sector security and resilience activities,</li><li>- provide knowledge, expertise, and assistance on request, and</li><li>- support timely sharing of threat indicators and defensive measures with the NCCIC.</li></ul>	<p>measures, and sharing information under the section. Requires a report with recommendations by the administrator to the President within one year of enactment on sharing by those institutions and use of shared information for network defense.</p> <p>Requires federal outreach to those institutions to encourage them to exercise the authorities provided under the section.</p> <p><b>‘Sec. 111(a)(2)’</b> 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. 12.]</p> <p>[Note: For other provisions of ‘Sec. 111(a)(2)’, see pp. 10 and 19.]</p> <p><b>‘(b) Definitions’</b></p> <p>Defines the following terms by reference to Sec. 110 of the title: <i>Appropriate Federal Entities</i>, <i>Cyber Threat Indicator</i>, <i>Defensive Measure</i>, <i>Federal Entity</i>, and <i>Non-Federal Entity</i>.</p> <p><b>(b) Submittal to Congress</b></p> <p>Requires that the procedures developed by the DNI be submitted to Congress within 90 days of enactment of the title.</p> <p><b>(c) Table of Contents Amendment</b></p> <p>Revises the table of contents of the National Security Act of 1947 to reflect the addition of ‘Sec. 111’.</p>

NCPAA—Title II	PCNA—Title I
<p data-bbox="191 520 711 548"><b>‘(i) Voluntary Information Sharing Procedures’</b></p> <p data-bbox="191 646 792 919"><b>‘(1)’</b> 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.</p> <p data-bbox="191 940 792 1129"><b>‘(2)’</b> 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.</p> <p data-bbox="191 1161 792 1381">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 31<sup>st</sup> 2014.” Also stipulates that an agreement is not required for an entity to be in compliance with ‘(i).’</p>	<p data-bbox="829 279 1401 390"><b>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</b></p> <p data-bbox="829 405 1328 432"><b>(a) Requirement for Policies and Procedures</b></p> <p data-bbox="829 447 1360 499"><b>(1)</b> Adds new subsections to ‘Sec. 111’ of the National Security Act of 1947</p> <p data-bbox="829 520 1369 632"><b>‘(b) Policies and Procedures for Sharing with the Appropriate Federal Entities Other Than the Department of Defense or the National Security Agency’</b></p> <p data-bbox="829 646 1425 730"><b>‘(1)’</b> 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 data-bbox="829 1398 1425 1696"><b>‘(2)’</b> requires that they be developed in accordance with the privacy and civil liberties guidelines under Sec. 104(b) of the title, and ensure<ul data-bbox="829 1482 1425 1696" style="list-style-type: none"><li>- real-time sharing of indicators from nonfederal entities with appropriate federal entities except DOD,</li><li>- receipt without delay except for good cause, and</li><li>- provision to all relevant federal entities,</li><li>- audit capability, and</li><li>- appropriate sanctions for federal personnel who knowingly and willfully use shared information other than in accordance with the title.</li></ul></p> <p data-bbox="829 1717 1409 1801"><b>(2)</b> 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.</p> <p data-bbox="829 1818 1393 1869"><b>(c) National Cyber Threat Intelligence Integration Center</b></p>



NCPAA—Title II	PCNA—Title I
	<p>(1) Adds a new section to the National Security Act of 1947.</p> <p><b>‘Sec. 119B. Cyber Threat Intelligence Integration Center’</b></p> <p><b>‘(a) Establishment’</b></p> <p>Establishes the CTIIC within the ODNI.</p> <p><b>‘(b) Director’</b></p> <p>Creates a director for the CTIIC, to be appointed by the DNI.</p> <p><b>‘(c) Primary Missions’</b></p> <p>Specifies the missions of the CTIIC with respect to cyberthreat intelligence as</p> <ul style="list-style-type: none"><li>- serving as the primary federal organization for analyzing and integrating it,</li><li>- ensuring full access and support of appropriate agencies to activities and analysis,</li><li>- disseminating analysis to the President, appropriate agencies, and Congress,</li><li>- coordinating agency activities, and</li><li>- conducting strategic federal planning.</li></ul> <p><b>‘(d) Limitations’</b></p> <p>Requires that the CTIIC</p> <ul style="list-style-type: none"><li>- have no more than 50 permanent positions,</li><li>- may not augment staff above that limit in carrying out its primary missions, and</li><li>- be located in a building owned and operated by an element of the IC,</li></ul> <p>(4) revises the table of contents of the National Security Act of 1947.</p>
<p><b>‘(3) Information Sharing Authorization’</b></p> <p>Permits nonfederal entities to share, for cybersecurity purposes, cyber threat indicators, and defensive measures, <u>from their own information systems</u> or those of other entities upon written consent, with other nonfederal entities or <u>the NCCIC</u>,</p> <p>notwithstanding any other provision of law, except that recipients must comply with lawful restrictions on sharing and use imposed by the source.</p> <p>Requires reasonable efforts by nonfederal and federal entities, <u>prior to sharing</u>, to safeguard personally identifying information from unintended disclosure or unauthorized access or acquisition and remove or <u>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><b>Sec. 103(c) Authorization for Sharing or Receiving Cyber Threat Indicators or Defensive Measures</b></p> <p>(1) permits nonfederal entities to share, for cybersecurity purposes <u>and consistent with privacy requirements under (d)(2) and protection of classified information, lawfully obtained</u> cyber threat indicators or defensive measures with other nonfederal entities or <u>appropriate federal entities except DOD</u>,</p> <p>(1,2) [Similar to NCPAA].</p> <p><b>(d) Protection and Use of Information</b></p> <p>(2) requires reasonable efforts by nonfederal entities, <u>before sharing a threat indicator</u>, to</p> <p>remove information <u>reasonably believed to be personal</u> or personally identifying of a specific person <u>not directly related</u> to a cybersecurity <u>threat</u>, or implement a technical capability for removing such information.</p>

NCPAA—Title II	PCNA—Title I
<p>Stipulates that nothing in ‘(3)’</p> <ul style="list-style-type: none"> <li>- limits or modifies an existing information sharing relationship or prohibits or requires a new one,</li> </ul> <ul style="list-style-type: none"> <li>- limits otherwise lawful activity, or</li> <li>- impacts or modifies existing procedures for reporting criminal activity to appropriate law enforcement authorities, or participating in an investigation.</li> </ul> <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><b>‘(4) Network Awareness Authorization’</b></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> <ul style="list-style-type: none"> <li>- its own information systems,</li> <li>- with written consent, information systems of a nonfederal or federal entity, or</li> <li>- the contents of such systems.</li> </ul> <p>Stipulates that nothing in ‘(4)’</p> <ul style="list-style-type: none"> <li>- authorizes <u>network awareness</u> other than as provided in the <u>section</u>, or</li> <li>- limits otherwise lawful activity.</li> </ul> <p><b>‘(5) Defensive Measure Authorization’</b></p> <p>Permits <u>nonfederal, nongovernment</u> entities to operate defensive measures, for cybersecurity purposes and to protect rights or property, that are <u>applied to</u></p> <ul style="list-style-type: none"> <li>- its own information systems,</li> <li>- with written consent, information systems of a nonfederal or federal entity, or</li> <li>- the contents of such systems,</li> </ul> <p>notwithstanding any other provision of law, except that measures may not be used except as authorized in <u>the</u></p>	<p><b>Sec. 109. Construction and Preemption</b></p> <p><b>(f) Information Sharing Relationships</b></p> <p>Stipulates that nothing in <u>the title</u></p> <ul style="list-style-type: none"> <li>- (1) limits or modifies an existing information sharing relationship or (2) prohibits or requires a new one,</li> </ul> <p><b>Sec. 103(c)(3)</b> stipulates that nothing in (c)</p> <ul style="list-style-type: none"> <li>- authorizes information sharing other than as provided in (c),</li> <li>- permits unauthorized sharing of classified information,</li> <li>- authorizes federal surveillance of any person,</li> <li>- 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,</li> <li>- prohibits otherwise lawful sharing by a nonfederal entity of indicators or defensive measures with DOD, or</li> </ul> <p>[Similar to NCPAA]</p> <p><b>(a) Authorization for Private-Sector Defensive Monitoring</b></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> <ul style="list-style-type: none"> <li>- authorizes <u>monitoring</u> other than as provided in the <u>title</u>,</li> </ul> <p>[Similar to NCPAA] or</p> <ul style="list-style-type: none"> <li>- authorizes federal surveillance of any person.</li> </ul> <p><b>(b) Authorization for Operation of Defensive Measures</b></p> <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> <p>with written authorization, information systems of a nonfederal or federal entity, or</p> <p>(1) notwithstanding any other provision of law, except that (3) measures may not be used except as authorized in <u>(b)</u>,</p>

NCPAA—Title II	PCNA—Title I
<p><u>section</u>, and <u>'(5)'</u> does not limit otherwise lawful activity.</p> <p>[No Corresponding Provision; however, the definition of defensive measure in Sec. 202(a) includes a similar restriction; see p. 8.]</p> <p><b>'(6) Privacy and Civil Liberties Protections'</b></p> <p>Requires the <u>U/S-CIP</u>, 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 section.</p> <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</p> <ul style="list-style-type: none"> <li>- be consistent with DHS FIPPs,</li> </ul> <p>- "<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,</p> <ul style="list-style-type: none"> <li>- <u>minimize</u> impacts on privacy and civil liberties,</li> <li>- 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,</li> <li>- include requirements to safeguard from unauthorized access or acquisition cyber threat indicators and <u>defensive measures</u> retained by the NCCIC, <u>identifying specific persons, including proprietary or business-sensitive information</u>,</li> <li>- protect the confidentiality of cyber threat indicators and <u>defensive measures</u> associated with specific persons, to the greatest extent practicable,</li> <li>- ensure that relevant constitutional, legal, and privacy</li> </ul>	<p>and <u>(b)</u> does not limit otherwise lawful activity.</p> <p><b>(2)</b> 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><b>(e) No Right or Benefit</b></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><b>Sec. 104(b) Privacy and Civil Liberties</b></p> <p><b>(1)</b> requires the <u>AG</u>, in <u>consultation</u> with appropriate federal agency heads 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 threat indicators obtained through the title's provisions.</p> <p><b>(2)</b> requires that, consistent with the need for protection of information systems and <u>threat</u> mitigation, the guidelines</p> <ul style="list-style-type: none"> <li>- 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"],</li> <li>- limit receipt, retention, use, and <u>dissemination</u> of cybersecurity threat indicators <u>containing personal information of or identifying specific persons</u>,</li> </ul> <p>including by establishing processes for prompt destruction of information known not to be directly related to uses for cybersecurity purposes, setting limitations on retention of indicators, and notifying recipients that indicators may be used only for cybersecurity purposes,</p> <ul style="list-style-type: none"> <li>- <u>limit</u> impacts on privacy and civil liberties of federal activities under the title, including guidelines for removal of personal and personally identifying information handled by federal entities under the title,</li> <li>- include requirements to safeguard from unauthorized access or acquisition cyber threat indicators <u>containing personal information of or identifying specific persons</u>,</li> </ul> <ul style="list-style-type: none"> <li>- be consistent with other applicable provisions of law,</li> </ul>

NCPAA—Title II	PCNA—Title I
protections are observed.	
Stipulates that the U/S-CIP may consult with NIST in developing the policies and procedures.	<ul style="list-style-type: none"><li>- include procedures to notify entities if a federal entity receiving information knows that it is not a cyber threat indicator,</li><li>- include steps to ensure that dissemination of indicators is consistent with the protection of classified and other sensitive national security information.</li></ul>
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.	<p>(3) requires the AG to submit to Congress interim guidelines within 90 days of enactment and final guidelines within 180 days.</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.	
Requires the DHS CPO to <ul style="list-style-type: none"><li>- monitor implementation of the policies and procedures,</li><li>- submit to Congress an annual review on their effectiveness,</li><li>- 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,</li><li>- regularly review and update impact assessments as appropriate to ensure that all relevant protections are followed, and</li></ul>	
- ensure appropriate sanctions for DHS personnel who knowingly and willfully conduct unauthorized activities under the section.	<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>
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><b>Sec. 107. Oversight of Government Activities</b></p> <p><b>(b) Reports on Privacy and Civil Liberties.</b></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>
- 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,	

NCPAA—Title II	PCNA—Title I
<ul style="list-style-type: none"><li>- a list of federal <u>agencies</u> receiving the <u>information</u>.</li><li>- review of sharing of <u>information</u> within the federal government to identify inappropriate <u>stovepiping</u> of shared information, and</li><li>- recommendations for improvements or modifications to <u>sharing</u> under the <u>section</u>.</li></ul>	<ul style="list-style-type: none"><li>- a list of federal <u>entities</u> receiving the <u>indicators</u>.</li><li>- review of sharing of <u>indicators</u> among federal entities to identify inappropriate <u>barriers</u> to sharing information,</li><li>- procedures for sharing information and removal of personal and identifying information, and incidents involving improper treatment of it, and</li><li>- recommendations for improvements or modifications to <u>authorities</u> under the <u>title</u>.</li></ul> <p>Requires that the reports be submitted in unclassified form but permits a classified annex.</p> <p>Requires public availability of unclassified parts of the reports.</p> <p><b>(1)</b> adds a new paragraph to Sec. 1061(e) of the Intelligence Reform and Terrorism Prevention Act of 2004:</p>
<p>Requires the <u>DHS CPO and Chief Civil Rights and Civil Liberties Officer</u>, in consultation with the <u>PCLOB</u>, the <u>DHS IG</u>, and senior privacy and civil liberties officers of each federal agency receiving indicators or defensive measures shared with the <u>NCCIC</u>, to</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>recommendations to minimize or mitigate such impacts.</p>	<p><b>‘(3)’</b> requires the <u>PCLOB</u> to</p> <p>submit a biennial report to Congress and the President</p> <p>assessing impacts of activities under the title on and sufficiency of policies, procedures, and guidelines in addressing concerns about privacy and civil liberties, including</p> <p>recommendations for improvements or modifications to authorities under the title.</p> <p>Requires that the reports be submitted in unclassified form but permits a classified annex.</p> <p>Requires public availability of unclassified parts of the reports.</p>
	<p><b>(a) Biennial Report on Implementation</b></p> <p><b>(1)</b> Adds to ‘Sec. 111’ of the National Security Act</p> <p><b>‘(c) Biennial Report on Implementation’</b></p> <p><b>‘(1)’</b> requires the DNI to submit a report to Congress on implementation of the title, <b>(2)</b> within one year of enactment and <b>‘(1)’</b> at least biennially thereafter, <b>‘(2)’</b> including</p> <ul style="list-style-type: none"><li>- review of types of indicators shared with the federal government,</li><li>- 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,</li><li>- assessment of sufficiency of policies, procedures, and guidelines to ensure effective and responsible sharing under Sec. 4 [sic] of PCNA,</li><li>- sufficiency of procedures under Sec. 3 [sic] for timely sharing, [Note: References ‘Sec. 111(a)(1)’ as added by the title; see p. 10],</li></ul>

NCPAA—Title II	PCNA—Title I
	<ul style="list-style-type: none"><li>- appropriateness of classification of indicators and accounting of security clearances authorized,</li><li>- federal actions taken based on shared indicators, including appropriateness of subsequent use or dissemination under the title,</li><li>- 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</li><li>- 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.</li><li>-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 presumably to Sec. 103 and 104 respectively.]</li></ul> <p><b>'(3)'</b> permits reports to include recommendations for improvements or modifications to authorities and processes under the title.</p> <p><b>'(4)'</b> requires that the reports be submitted in unclassified form but permits a classified annex.</p> <p><b>'(5)'</b> requires public availability of unclassified parts of the reports.</p>
<p><b>'(7) Uses and Protection of Information'</b></p>	<p><b>Sec. 103. Authorizations for Preventing, Detecting, Analyzing, and Mitigating Cybersecurity Threats</b></p> <p><b>(d) Protection and Use of Information</b></p>
<p><b>[Nonfederal Entities]</b></p>	<p><b>(3)</b> permits a nonfederal entity [Note: <u>including government entities</u>], for a cybersecurity purpose, to</p>
<p>Permits a nonfederal, <u>nongovernment</u> entity that shares indicators or defensive measures with the NCCIC to</p>	<p>use indicators or defensive measure shared or received under</p>
<p>use, retain, or disclose indicators and defensive measures, solely for cybersecurity purposes.</p>	<p>(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</p>
<p>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.</p>	<p>[See (2), p. 13, describing requirements for removal of personal information].</p>
<p>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.</p>	<p>further use, retention, or sharing subject to lawful restrictions by the sharing entity or otherwise applicable provisions of law.</p>
<p>Stipulates that the information shall be deemed voluntarily shared.</p>	
<p>Requires implementation <u>and utilization</u> of security controls to protect against unauthorized access or acquisition.</p>	<p><b>(1)</b> requires implementation of <u>appropriate</u> security controls to protect against unauthorized access or acquisition. [Note:</p>

NCPAA—Title II	PCNA—Title I
Prohibits use of such information to gain an unfair competitive advantage.	Also applies to nonfederal government entities.]
<b>[Federal Entities]</b>	<b>Sec. 104(d) Information Shared with or Provided to the Federal Government</b>
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	<b>(5)</b> 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
cybersecurity purposes.	a cybersecurity purpose,
[Note: Sec. 216 (see p. 28) permits use of information obtained from federal systems for investigating, prosecuting, disrupting, or otherwise responding to	responding to, investigating, prosecuting, or otherwise preventing or mitigating
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 <u>or</u> threats to physical safety, and	serious threats to minors, including sexual exploitation <u>and</u> 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.
	<b>'Sec. 111(a)(2)'</b> 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 or exclude such information.
Stipulates that the indicators and defensive measures shall be deemed voluntarily shared.	<b>Sec. 104(d)(3)</b> stipulates that the information shall be deemed voluntarily shared.
Requires implementation and utilization of security controls to protect against unauthorized access or acquisition.	<b>'Sec. 111(a)(2)'</b> 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.
	<b>Sec. 109(a) Prohibition of Surveillance</b>
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).	<b>Sec. 104(d)(3)</b> [Similar to NCPAA], and

NCPAA—Title II	PCNA—Title I
Prohibits federal use for regulatory purposes.	under nonfederal disclosure laws, except for those requiring disclosure in criminal prosecutions. [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 the title, the information be considered the commercial, financial, and proprietary information of the originating nonfederal source, when so designated by such source or nonfederal entity acting with written authorization from it.
Stipulates that the information is not subject to judicial doctrine or rules of federal entities on ex-parte communications.	(4) [Similar to NCPAA]
<b>[Nonfederal Government Entities]</b>	[Note: See also Nonfederal Entities, p. 18]
Permits state, local, and tribal government to use, retain, or further disclose indicators <u>or defensive measures</u> shared under the section solely for cybersecurity purposes.	<b>Sec. 103(d)(4)</b> permits state, local, and tribal government entities 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. 13, 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. 18.]
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.	(1) requires implementation of <u>appropriate</u> 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.
Prohibits use for regulation of lawful activities of nonfederal entities.	
<b>‘(8) Liability Exemptions’</b>	<b>Sec. 106. Protection from Liability</b> <b>(a) Monitoring of Information Systems</b>



NCPAA—Title II	PCNA—Title I
States that “no cause of action shall lie or be maintained in any court” against <u>nonfederal, nongovernment</u> entities for conducting network awareness under ‘(4)’ in accordance with the <u>section</u> or	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 title or
for sharing indicators or defensive measures under ‘(3),’ or a good-faith failure to act if sharing is done in accordance with the <u>section</u> .	<b>(b) Sharing or Receipt of Cyber Threat Indicators</b> for information sharing under Sec. 103(c) in accordance with the title, or a good-faith failure to act if sharing is done in accordance with the <u>title</u> .
Stipulates that nothing in the section	<b>(c) Willful Misconduct</b> <b>(1)</b> 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 <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
- undermines or limits availability of otherwise applicable common law or statutory defenses.	[Identical to NCPAA]
Establishes the burden of proof as clear and convincing evidence from the plaintiff of injury-causing gross negligence or willful misconduct,	<b>(2)</b> [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.	<b>(3)</b> [Similar to NCPAA].
<b>‘(9) Federal Government Liability for Violations of Restrictions on the Use and Protection of Voluntarily Shared Information’</b>	<b>Sec. 105. Federal Government Liability for Violations of Privacy or Civil Liberties</b>
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	<b>(a) In General</b> 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]
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	<b>(b) Venue</b> [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.
Sets the statute of limitations under ‘(i)’ at two years from the date on which the cause of action arises.	<b>(c) Statute of Limitations</b> 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 ‘(i)’ as the exclusive remedy for violation of <u>restrictions under ‘(i)(3),’ ‘(i)(6),’ or ‘(i)(7)(B)’</u> .	<b>(d) Exclusive Cause of Action.</b> Sets action under (d) as the exclusive remedy for federal violations under <u>the title</u> .
<b>‘(10) Anti-Trust Exemption’</b>	

**NCPAA—Title II**

**PCNA—Title I**

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.

**‘(I I) Construction and Preemption’**

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 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 federal or state law.

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 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 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 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 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.

Stipulates that nothing in the bill “shall be construed to permit price-fixing, allocating a market between competitors,

**Sec. 109(b) Otherwise Lawful Disclosures**

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 title 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.

**(e) Relationship to Other Laws**

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 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 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 title does not create liabilities for any nonfederal entities that choose not to engage in a voluntary activity authorized in the title.

**(j) Use and Retention of Information**

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.

NCPAA—Title II	PCNA—Title I
<p>monopolizing or attempting to monopolize a market, <u>boycotting</u>, or exchanges of price or cost information, customer lists, or information regarding future competitive planning.”</p> <p>Specifies that the <u>section</u> supersedes state and local laws relating to its provisions</p> <p>Requires the Secretary to develop policies and procedures for direct reporting by the NCCIC Director of significant risks and incidents.</p> <p>Requires the Secretary to build on existing mechanisms to promote public awareness about the importance of securing information systems.</p> <p>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.</p> <p>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.</p>	<p><b>(k) Federal Preemption</b></p> <p><b>(1)</b> specifies that the <u>title</u> supersedes state and local laws relating to its provisions.</p> <p><b>(2)</b> stipulates that the title does not supersede state and local laws on use of authorized law enforcement practices and procedures.</p> <p><b>(3)</b> 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.</p> <p><b>(d) Protection of Sources and Methods</b></p> <p>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, intelligence sources and methods, and U.S. national security.</p>
<p><b>Sec. 204. Information Sharing and Analysis Organizations</b></p> <p>Amends Sec. 212 of the HSA to</p> <p><b>(1)</b> broaden the functions of ISAOs to include cybersecurity risk and incident information beyond that relating to critical infrastructure, and</p> <p><b>(2)</b> add by reference the definitions of <i>cybersecurity risk</i> and <i>incident</i> in 6 U.S.C. 148(a).</p> <p><b>Sec. 205. Streamlining of Department of Homeland Security Cybersecurity and Infrastructure Protection Organization</b></p> <p><b>(a) Cybersecurity and Infrastructure Protection Directorate</b></p> <p>Renames the DHS National Protection and Programs</p>	

---

**NCPAA—Title II**

**PCNA—Title I**

---

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.

**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’**

---

**NCPAA—Title II**

**PCNA—Title I**

---

**‘(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,
- 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

---

**NCPAA—Title II**

**PCNA—Title I**

---

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

**‘(c) Coordination’**

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

**‘(d) Consultation’**

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

**(b) Clerical Amendment**

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

**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

NCPAA—Title II	PCNA—Title I
	<p>or prevent such threats to the U.S. private sector are degraded by delays in notification of the threats,</p> <p>(4) assessment of additional technologies or capabilities that would enhance the U.S. ability to prevent and respond to such threats, and</p> <p>(5) assessment of private-sector technologies or practices that could be rapidly fielded to assist the IC in preventing and responding to such threats.</p> <p><b>(c) Form of Report</b></p> <p>Requires that the report be unclassified, but may include a classified annex.</p> <p><b>(d) Public Availability of Report</b></p> <p>Requires that the unclassified portion of the report be publicly available.</p> <p><b>(e) Intelligence Community Defined</b></p> <p>Defines intelligence community as in 50 U.S.C. 3003.</p>
<p><b>Sec. 210. Assessment</b></p>	
<p>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.</p>	
<p><b>Sec. 211. Consultation</b></p>	
<p>Requires a report from the U/S-CIP on “the feasibility of a prioritization plan in the event of simultaneous multi-CI incidents.</p>	
<p><b>Sec. 212. Technical Assistance</b></p>	
<p>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.</p>	
<p><b>Sec. 213. Prohibition on New Regulatory Authority</b></p>	<p><b>Sec. 109(l) Regulatory Authority</b></p>
<p>Stipulates that the title does not grant DHS new authority to promulgate regulations or set standards relating to cybersecurity for nonfederal, nongovernmental entities.</p>	<p>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.</p>
<p><b>Sec. 214 Sunset</b></p>	
<p>Ends all requirements for reports in the title seven years after enactment.</p>	
<p><b>Sec. 215. Prohibition on New Funding</b></p>	
<p>Stipulates that the title does not authorize additional funds for implementation and must be carried out using available amounts.</p>	
<p><b>Sec. 216. Protection of Federal Information Systems</b></p>	
<p><b>(a) In General</b></p>	

NCPAA—Title II	PCNA—Title I
<p>Adds a new section to the HSA.</p>	
<p><b>‘Sec. 233. Available Protection of Federal Information Systems’</b></p>	
<p><b>‘(a) In General’</b></p>	
<p>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.</p>	
<p><b>‘(b) Activities’</b></p>	
<p>Authorizes the Secretary to</p>	
<p>- 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,</p>	
<p>- obtain assistance through agreements or otherwise from private entities for implementing technologies under ‘(a),’</p>	
<p>- use, retain, and disclose information obtained under this section only to protect federal systems and their contents or,</p>	
<p>with approval of the AG, to respond to violations of 18 U.S.C. 1030 [on computer fraud and related activities],</p>	<p>[Note: Sec. 104(d)(5) has related provisions for information shared with the federal government (see p. 19).]</p>
<p>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.</p>	
<p><b>‘(c) Conditions’</b></p>	
<p>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.</p>	
<p><b>‘(d) Limitation’</b></p>	
<p>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).’</p>	
<p><b>(b) Clerical Amendment</b></p>	
<p>Amends the table of contents of the act to include the new section.</p>	
<p><b>Sec. 217 Sunset</b></p>	<p><b>Sec. 112 Sunset</b></p>
<p>Terminates the provisions in the title seven years after enactment.</p>	<p>[Identical to NCPAA]</p>
<p><b>Sec. 218. Report on Cybersecurity Vulnerabilities of United States Ports</b></p>	
<p>Requires a report with recommendations from the Secretary</p>	



---

<b>NCPAA—Title II</b>	<b>PCNA—Title I</b>
<p>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.</p> <p><b>Sec. 219. Report on Cybersecurity and Critical Infrastructure</b></p> <p>Authorizes the Secretary to consult with sector-specific entities on a report to HSC and HSGAC on federally funded cybersecurity R&amp;D with private-sector efforts to protect privacy and civil liberties while protecting CI, including promoting R&amp;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.</p> <p><b>Sec. 220. GAO Report on Impact Privacy and Civil Liberties</b></p> <p>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.</p>	<p><b>Sec. 111. Comptroller General Report on Removal of Personal Identifying Information</b></p> <p><b>(a) Report</b></p> <p>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).</p> <p><b>(b) Form</b></p> <p>Requires that the report be unclassified but permits a classified annex.</p>

---

**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