Side-by-Side Comparison of House and Senate Cybersecurity Information Sharing Bills

The chart below compares selected provisions of three cybersecurity bills that have advanced in Congress this year. Senate bill S.754, entitled the Cybersecurity Information Sharing Act (CISA), was sponsored by Senate Select Committee on Intelligence Chairman Richard Burr (R-NC) and Vice Chairman Dianne Feinstein (D-CA), and passed the Senate on October 27, 2015. The House of Representatives passed two separate cybersecurity measures earlier in the year. The first bill, H.R.1560, entitled the Protecting Cyber Networks Act (PCNA), was introduced by House Permanent Select Committee on Intelligence Chairman Devin Nunes (R-CA). The second bill, H.R. 1731, entitled the National Cybersecurity Protection Advancement Act (NCPAA), was introduced by House Homeland Security Committee Chairman Michael McCaul (R-TX). Upon separate consideration and passage of each of these bills in the House, NCPAA was added to H.R.1560 as title II (with PCNA as title I), creating a single legislative measure in the House for cybersecurity going forward.

As the chart below describes, the three bills contain many similarities but also some key differences. All share the same goal of providing companies liability protections for sharing information with other companies and with the Federal government. PCNA and CISA are closer in language to each other than the NCPAA is to either of them, reflecting in part the emergence of PCNA and CISA from in the Intelligence Committees and NCPAA's emergence from the Homeland Security Committee. Consequently, where the PCNA and CISA would position multiple federal agency stakeholders as participating in the development and implementation of cyber information sharing, the NCPAA would designate the Department of Homeland Security's National Cybersecurity & Communications Integration Center (CCIC) as the "lead federal civilian interface" for information sharing and would assign greater duties to the Department overall. Other provisions vary across the bills, such as those extending liability protections to private entities sharing information. For example, NCPAA would provide liability protection to entities conducting network monitoring, sharing or receiving cyber threat info, or failing to act based on such sharing. PCNA would do the same, but would impose a good faith standard for a failure to act. PCNA and NCPAA would immunize all conduct short of willful misconduct, while CISA would preserve a cause of action for gross negligence.

The chart below does not attempt to summarize every aspect of these bills. Measures related to agencies reporting to Congress and other such provisions have been excluded.

CISA	PCNA	NCPAA
Information Sharing Procedures		
Requires the Director of National Intelligence (DNI), the Department of Homeland Security (DHS), the Department of Defense (DOD), and the Department of Justice (DOJ) to develop procedures to promote: 1. the timely sharing of classified and declassified cyber threat indicators in possession of the federal government with private entities, non-federal government agencies, or state, tribal, or local governments; 2. the sharing of unclassified indicators with the public; and 3. the sharing of cybersecurity threats with entities to prevent or mitigate adverse effects.	Requires the DNI to develop procedures to promote: 1. the timely sharing of classified and declassified cyber threat indicators in possession of the federal government with private entities, non-federal government agencies, or state, tribal, or local governments; and 2. the sharing of imminent or ongoing cybersecurity threats with such entities to prevent or mitigate adverse impacts.	Requires the National Cybersecurity & Communications Integration Center (CCIC) to be the lead federal civilian interface for multi-directional and cross-sector sharing of information related to cyber threat indicators, defensive measures, and cybersecurity risks for federal and non-federal entities. Expands the NCCIC's functions to include: 1. global cybersecurity with int'l partners; 2. info sharing across critical infrastructure sectors, incl. state and local gov. and businesses; 3. notification to Congress regarding retention or disclosure violations; 4. notification to non-federal entities of improper disclosures; and 5. participation in exercises run by DHS's National Exercise Program.
Information Sharing by Nonfederal Entities		
Permits private entities to monitor, and operate defensive measures to detect, prevent, or mitigate cybersecurity threats or security vulnerabilities on: (1) their own information systems; and (2) with	[Similar to CISA]	Authorizes non-federal entities (excluding state, local, or tribal governments) to conduct network awareness to scan, identify, acquire, monitor, log, or analyze information, or to operate defensive

CISA	PCNA	NCPAA
authorization and written consent, the information systems of other private or government entities. Authorizes such entities to monitor information that is stored on, processed by, or transiting such monitored systems.		measures, on the information systems of entities that provide consent.
Allows entities to share and receive indicators and defensive measures with other entities or the federal government. Requires recipients to comply with lawful restrictions that sharing entities place on the sharing or use of shared indicators or defensive measures.	Allows non-federal entities to share and receive indicators or defensive measures with other non-federal entities or specifically designated federal entities, but does not authorize non-federal entities to share directly with components of the Department of Defense (DOD), including the National Security Agency (NSA). Allows otherwise lawful sharing by non-federal entities of indicators or defensive measures with DOD or the NSA. Requires recipients to comply with lawful restrictions that sharing entities place on the sharing or use of shared indicators or defensive measures.	Allows non-federal entities to share with other non-federal entities or the NCCIC any indicators or defensive measures obtained from: (1) their own information systems; or (2) the information systems of other federal or non-federal entities, with written consent.
Requires the federal government and entities monitoring, operating, or sharing indicators or defensive measures: 1. to utilize security controls to protect against unauthorized access or acquisitions, and 2. prior to sharing an indicator, to	Requires non-federal entities monitoring, operating, or sharing indicators or defensive measures: 1. to implement security controls to protect against unauthorized access or acquisitions; and 2. prior to sharing an indicator, to	Requires entities, prior to sharing, to take reasonable efforts to: 1. exclude information that can be used to identify specific persons and that is unrelated to cybersecurity risks or incidents, and

CISA	PCNA	NCPAA
remove personal information of or identifying a specific person not directly related to a cybersecurity threat.	take reasonable efforts to remove information that the non-federal entity reasonably believes to be personal information of, or information identifying, a specific person not directly related to a cybersecurity threat. Prohibits defensive measures from being used to destroy, render unusable or inaccessible, or substantially harm an information system that is not owned by: (1) the operator of the defensive measure, or (2) an entity that authorizes the operation of defensive measures on its systems. Requires the Small Business Administration (SBA) to provide assistance to small businesses and financial institutions to monitor information systems, operate defensive measures, and share and receive indicators and defensive measures. Directs the SBA to submit to the President a report regarding the degree to which small businesses and financial institutions are able to engage in such sharing. Requires the federal government to conduct outreach to encourage such businesses and	2. safeguard information that can be used to identify specific persons from unintended disclosure or unauthorized access or acquisition.

CISA	PCNA	NCPAA
	institutions to engage in those activities.	
Exempts from antitrust laws private entities that, for cybersecurity purposes, exchange or provide: (1) cyber threat indicators; or (2) assistance relating to the prevention, investigation, or mitigation of cybersecurity threats. Makes such exemption inapplicable to price-fixing, allocating a market between competitors, monopolizing or attempting to monopolize a market, boycotting, or exchanges of price or cost information, customer lists, or information regarding future competitive planning.		[Similar to CISA]
Information Sharing by the Federal Government		
Directs DHS to develop a process within DHS for the federal government to: 1. Accept cyber threat indicators and defensive measures from any entity in real time, and 2. Ensure that appropriate federal entities receive the shared indicators in an automated manner through that real-time process. Requires DHS to certify to Congress that the DHS sharing capability is fully operational	Directs the President to report on procedures for the receipt of cyber threat indicators and defensive measures by the federal government and requires the procedures to ensure: 1. Indicators shared by a non-federal entity with the DOC, DOE, DHS, DOJ, Treasury, and the DNI (but not DOD, including the NSA) are shared in real time with all appropriate federal entities; 2. Indicators are provided to other	Requires the Under Secretary for Cybersecurity and Infrastructure Protection to develop capabilities that make use of existing industry standards to advance implementation of automated mechanisms for the timely sharing of indicators and defensive measures to and from the NCCIC and with federal agencies designated as sector specific agencies for critical infrastructure sectors. Directs the Under Secretary, every six

CISA	PCNA	NCPAA
before the process is implemented. Directs DOJ to develop, and make publicly available, guidelines to assist entities in sharing indicators with the federal government, including guidance for identifying and protecting personal information.	relevant federal entities; 3. An audit capability; and 4. Sanctions for unauthorized use of info by federal personnel	months, to provide Congress with progress reports regarding the development of such capabilities.
Requires DOJ to promulgate and periodically review privacy and civil liberties guidelines to limit receipt, retention, use, and dissemination of personal or identifying information. Provides for the guidelines to include steps to make dissemination of cyber threat indicators consistent with the protection of classified and other sensitive national security information.	Requires DOJ to develop and periodically review privacy and civil liberties guidelines to govern the receipt, retention, use, and dissemination of cyber threat indicators by federal entities, including guidelines to ensure that personal information of, or information identifying, specific persons is properly removed from information received, retained, used, or disseminated by a federal entity.	Directs the Under Secretary to establish and annually review privacy and civil liberties policies governing the receipt, retention, use, and disclosure of cybersecurity information shared with the NCCIC. Provides for such policies to apply only to DHS. Requires the Chief Privacy Officer to: • monitor implementation of privacy and civil liberties policies; • update privacy impact assessments on a regular basis to ensure privacy protections are followed; • work with Under Secretary to carry out notifications to Congress and non-federal entities; • ensure appropriate sanctions for DHS officers, employees, or

CISA	PCNA	NCPAA
		agents who intentionally or willfully conduct activities in an unauthorized manner.
Use of Information by Federal Government		
Authorizes indicators and defensive measures to be disclosed to, retained by, and used by, consistent with otherwise applicable federal law, any federal agency or federal government agent solely for: • protecting a system or info from a cybersecurity threat or security vulnerability or identifying the source of a cybersecurity threat; • responding to, or otherwise preventing or mitigating, a serious threat to a minor or an imminent threat of death, serious bodily harm, or serious economic harm, including a terrorist act or a use of a weapon of mass destruction; or • preventing, investigating, disrupting, or prosecuting an offense arising out of an imminent threat of death, serious bodily harm, or serious economic harm, as well as offenses relating to serious violent felonies, fraud and identity theft, espionage and censorship, or trade secrets.	[Substantially similar to CISA]	Authorizes the Secretary to retain, use, and disclose information obtained through the conduct of activities authorized under this section only to protect federal agency information and information systems from cybersecurity risks, or, with DOJ approval and if disclosure of such information is not otherwise prohibited by law, to law enforcement only to investigate, prosecute, disrupt, or otherwise respond to: • criminal computer fraud; • an imminent threat of death or serious bodily harm; • a serious threat to a minor, including sexual exploitation or threats to physical safety; or • an attempt or conspiracy to commit any of such offenses.

CISA	PCNA	NCPAA
• identifying the use of an information system by a foreign adversary or terrorist;		
Private Cause of Action		
N/A	Allows a person to bring a private cause of action against the federal government if an agency intentionally or willfully violates DOJ's privacy and civil liberties guidelines.	Establishes a private cause of action that a person may bring against the federal government if a federal agency intentionally or willfully violates restrictions on the use and protection of voluntarily shared indicators or defensive measures.
Liability Protection		
Provides liability protections to entities that: 1. Monitor information systems, or 2. Share or receive indicators or defensive measures, provided that it is done consistent with procedures and exceptions set forth by DHS.	Provides liability protections to: 1. Private entities that monitor information systems; or 2. Non-federal entities that share, receive, or fail, in good faith, to act upon shared indicators or defensive measures. Prohibits liability protections from being construed to apply to willful misconduct.	Provides liability protections to non-federal entities (excluding state, local, or tribal governments) acting in accordance with this section that: 1. Conduct network awareness, or 2. Share indicators or defensive measures or that fail to act based on such sharing. Prohibits such liability protections from being construed to apply to willful misconduct.
Surveillance		
Prohibits this Act from being construed to	Prohibits the Act from being construed to: 1. Authorize the fed gov. to conduct surveillance of a person or allow	Prohibits federal entities from using shared indicators or defensive measures to

CISA	PCNA	NCPAA
permit the federal government to require an entity to provide information to the federal government.	the intelligence community to target a person for surveillance; 2. Limit lawful disclosures of communications or records, including reporting of known or suspected criminal activity, by a non-federal entity to another non-federal entity or the fed gov.; or 3. Permit the fed gov. to require a non-federal entity to provide info to the fed gov.	engage in surveillance or other collection activities for the purpose of tracking an individual's personally identifiable information, except for authorized purposes. Bars the federal government from using such information for regulatory purposes. Prohibits the Act from being construed to permit the federal government to require a non-federal entity to provide information to a federal entity.
Miscellaneous		
	Establishes within the Office of the Director of National Intelligence a Cyber Threat Intelligence Integration Center (CTIIC) to serve as the primary organization within the federal government for analyzing and integrating all intelligence possessed or acquired by the United States pertaining to cyber threats. Requires the CTIIC to: (1) ensure that appropriate agencies receive all-source intelligence support to execute cyber threat intelligence activities and perform independent, alternative analyses; (2) disseminate threat analysis to the President, federal agencies, and Congress; and (3) coordinate federal cyber threat	Requires DHS to establish a National Cybersecurity Preparedness Consortium to: • train state and local first responders and officials to prepare for and respond to cyber attacks, • develop a curriculum utilizing the DHS-sponsored Community Cyber Security Maturity Model, • provide technical assistance, • conduct cybersecurity training and simulation exercises, • coordinate with the NCCIC to help states and communities develop information sharing programs, and • coordinate with the National

CISA	PCNA	NCPAA
	intelligence activities and conduct strategic planning.	Domestic Preparedness Consortium to incorporate cybersecurity emergency responses into existing state and local emergency management functions.