	Safeguards for privacy and civil liberties	Preservation of long-standing, respective roles and missions of civilian and intelligence agencies	Provisions for appropriate sharing with targeted liability protections	Other considerations
Why it matters	The White House has pledged to veto legislation that does not require industry and government to "minimize and protect personally identifiable information" and doesn't have "clear legal protections and independent oversight." Cybersecurity legislation should not permit private entities or the government to distribute users' personal information that is unrelated to any cybersecurity threat. The legislative proposals enable companies to send "cyber threat indicators" to government agencies, a term each bill defines differently. Most of the laws risk user privacy by enabling the overbroad collection of identifying information by the government. The laws also largely have ineffective mechanisms for oversight. All of the bills fail to provide adequate transparency by creating unnecessary exemptions from open government laws.	The White House has explained that "sharing must be consistent with...the cybersecurity responsibilities of the agencies involved." As such, it is necessary that cybersecurity information only be used for cybersecurity purposes and only further disseminated to other government entities when necessary to fulfill a specific, identified goal. While these proposals are intended to enhance cybersecurity capabilities, practically speaking they have been labeled "cyberveillance" because they increase the amount of personal information that the government can receive and retain. While the bills mostly assign primary responsibility for carrying out their authorities to the Department of Homeland Security, a civilian government agency, they also require information be immediately forwarded to other agencies, including the NSA, one of the least transparent or accountable organizations in government.	The White House has said it was unacceptable for a law to contain broad liability limitations. The White House has also said that "adequate oversight or accountability measures" are "necessary to ensure that the data is used only for appropriate purposes." Liability protections protect companies who transmit information to government with disregard for its impact on the privacy of users. Compounding the problem, the bills pre-empt other privacy laws.	Outside of the three reasons the White House previously gave for threatening to veto "information sharing" legislation, the bills all contain other provisions that intrude upon privacy, harm digital security, and limit public transparency. For example, most of the bills would broadly authorize "defensive measures," measures that extend outside of an entities own system to that of another. The language of defensive measure provisions is often so broad as to forgive entities that cause harm or interfere with others' networks.

	Safeguards for privacy	Preservation of long-	Provisions for	Other

	and civil liberties	standing, respective roles and missions of civilian and intelligence agencies	appropriate sharing with targeted liability protections	considerations
Cyber Threat Sharing Act (CTSA) & President Obama's legislative proposal **Citation:** S. 456 **Status:** Introduced in the Senate; Referred to the Senate Committee on Homeland Security and Governmental Affairs **URL** CTSA: https://www.congress.gov/bill/114th-congress/senate-bill/456 President Obama's proposal: https://www.whitehouse.gov/sites/default/files/omb/legislative/letters/updated-information-sharing-legislative-proposal.pdf	Grade: [neutral] The Cyber Threat Sharing Act ("CTSA") closely mirrors President Obama's cybersecurity legislative proposal. Notwithstanding any current law, both proposals allow companies to share "cyber threat indicators" that are "necessary to indicate, describe, or identify" specified behavior. Information only becomes a cyber threat indicator if the entity makes "reasonable efforts" to remove information that identifies specific persons reasonably believed to be unrelated to the cybersecurity risk. Cyber threats do not include exceeding authorized access if based solely on violations of terms of service. Entities are also required to make reasonable efforts to remove identifying information upon receipt of information. Companies would have to comply with reasonable restrictions placed on subsequent disclosure or retention — providing some control over information shared between companies. The CTSA requires the Department of Homeland Security, in consultation with relevant agencies and the Privacy and Civil Liberties Oversight Board, to develop policies on "retention, use, and disclosure" of cyber threat indicators. Each agency would provide oversight of its privacy protections. The Privacy Officers at the Department of Homeland Security and Department of Justice would also be required to submit an annual report assessing the privacy and civil liberties impact of the program and a biannual report, which would describe the effectiveness and compliance of the program.	X Both the CTSA and the White House proposals designate the Department of Homeland Security, through the National Cybersecurity and Communications Integration Center (NCCIC), as the agency in control of the information sharing program, to disseminate through a portal all received information with other entities in "as close to real time as practicable", including with the NSA. Language in the law that codifies the NCCIC provides a broad definition of "cybersecurity incident," included in the definition of "cybersecurity purpose," to enable law enforcement to use shared information to investigate any crime. The bills also permit private entities to disclose information in order to report certain crimes unrelated to cybersecurity. The law requires that guidelines for law enforcement use of cyber threat indicators be created and, to the extent feasibly possible, to be posed online.	XX The White House proposal and the Cyber Threat Sharing Act both provide absolute civil and criminal liability protection for entities making disclosures under the rules of the Act, even for willful misconduct. The liability protection covers sharing of information with Information Sharing and Analysis Organizations (ISAOs) — private or public entities that self-certify that they have adopted privacy best practices. The liability protection also protects against regulatory action. A narrow provision orders the development of penalties for government agents or employees that violate the receipt, retention, and disclosure requirements, but no other redress is provided. CTSA provides broad liability protection for entities which act in "good faith."	[neutral] The CTSA would sunset without reauthorization after five years, while President Obama's proposal would not (one of only a few distinctions between the proposals). While the sunset would provide an opportunity to debate the program's privacy impact and usefulness, debate would be limited without stronger transparency provisions. The bill, and President Obama's proposal, would both reinforce the role of Information Sharing and Analysis Organizations (ISAOs), public or private entities that will analyze and share cybersecurity information. ISAOs would only have to self-certify that they are compliant with best practices. The bill also exempts shared information from both federal and state freedom of information requirements. CTSA does not include a defensive measures provision.

	Safeguards for privacy and civil liberties	Preservation of long-standing, respective roles	Provisions for appropriate sharing with	Other considerations

		and missions of civilian and intelligence agencies	targeted liability protections	
Cybersecurity Information Sharing Act (CISA) **Citation:** S. 754 **Status:** Introduced in the Senate; Marked up by Senate Intelligence Committee and placed on Senate legislative calendar **URL** https://www.congress.gov/bill/114th-congress/senate-bill/754	Grade: X The Cybersecurity Information Sharing Act ("CISA") would allow companies to send to government agencies, notwithstanding any other law, a broad range of information, namely anything "necessary to describe or identify," among other things, "any...attribute of a cybersecurity threat," which excludes constitutionally protected activity. Unlike other bills, the definition of what can be shared does not exclude personal information, though the bill separately requires companies to strip personal or identifying information (or use an automated process to do so). However, this requirement only applies if the entity knows about the presence of the information "at the time of sharing." The bill would require the Attorney General, in consultation with other agencies, to develop guidelines governing the "receipt, retention, use and dissemination of cyber threat indicators" with requirements to safeguard personal or identifying information. The procedures are required to be consistent with Fair Information Practice Principles (FIPPS) as developed by DHS under the Privacy Act of 1974 (though other bills use another formulation of the FIPPS that are more robust). While industry would be consulted in the development of these guidelines, there is no further requirement for public or civil society consultation. The bill would require several biennial reports, including from the Privacy and Civil Liberties Oversight Board, focusing on, among a number of other things, the impact of cyber threat indicators on privacy and civil liberties.	XX CISA requires that the Department of Homeland Security, as the agency identified as in control of cybersecurity operations, immediately share all received information with other entities, including the NSA. Sharing must be done in accordance with Fair Information Practices, as set out in the National Strategy for Trusted Identities in Cyberspace, and sharing practices must have an audit capability. The bill allows shared information to be used by law enforcement to investigate a number of non-cybersecurity related crimes, such as economic harm or crimes under the espionage act, which is frequently used to target journalists and whistleblowers.	X CISA provides broad liability protection for companies that share cyber threat indicators or defensive measures if conducted in accordance with the bill, unless the company acts with willful misconduct or gross negligence. The bill does not require that companies act in good faith and it does not provide a cause of action for companies whose sharing would qualify as willful misconduct.	XX CISA's defensive measures provision prohibits "substantial harm" to others' networks, leaving the possibility of measures that cause a significant degree of harm judged "non-substantial". The bill also includes an unprecedented modification to the Freedom of Information Act (FOIA) that prohibits the disclosure of information shared under the law, as well as a separate, non-discretionary exemption for information and defensive measures shared and exemptions from all state open government laws. The bill explicitly does not pre-empt state laws.

	Safeguards for privacy and civil liberties	Preservation of long-standing, respective roles and missions of	Provisions for appropriate sharing with targeted	Other considerations

		civilian and intelligence agencies	liability protections	
Cyber Intelligence Sharing and Protection Act (CISPA) **Citation:** H.R. 234 **Status:** Introduced in the House; Referred to the House Judiciary Subcommittee on the Constitution and Civil Justice **URL** https://www.congress.gov/bill/114th-congress/house-bill/234/text	Grade: XX The Cybersecurity Information Sharing and Protection Act ("CISPA") considers the sharing of "cyber threat information" (instead of "indicators"), the definition of which encompasses potentially more personal information than in the other bills, including information *pertaining* to elements of cybersecurity threats. Terms of service or licensing violations are explicitly excluded. However, unlike the other bills, information does not have to be necessary to facilitate a reaction (e.g., to indicate or describe the threat). CISPA allows information to be sent to the government regardless of if it would otherwise violate an existing law. In addition, CISPA weakly requires only "appropriate anonymiziation or minimization," but fails to identify a specific standard for the anonymization or explicitly require the removal of personal or unrelated information. Pursuant to the bill, DHS, in consultation with other government entities, would establish privacy and civil liberties guidelines in order to reasonably limit the unnecessary retention or use of personal information. CISPA does provide some protection against government use of certain types of data, including book and firearm sales and educational and medical records. The Inspector Generals of relevant agencies and Officer for Civil Rights and Liberties at the Department of Homeland Security, in consultation with the Privacy and Civil Liberties Board and other oversight entities, are required to submit separate annual reports to Congress. Each report could contain a classified annex.	XX CISPA requires that any agency that receives information shares it with other agencies, including defense agencies, in real time. CISPA would allow cyber threat information to be used to investigate crimes, even if there is no evidence of imminent harm, providing law enforcement more leeway in using and storing personal information. The bill does require that agencies receiving information not disseminate it to other agencies if sharing would "undermine the purpose" for which it was originally shared. CISPA prohibits the Department of Defense or NSA from using shared information to target U.S. persons, however it is silent on targeting by other US. agencies or of non-U.S. persons.	X CISPA provides broad liability protection for entities which act in "good faith." Uniquely, the protection extends to decisions made based upon information that is received under the bill. CISPA includes a private right of action against federal departments or agencies that violate the rules regarding protection of information. However, the cause of action is the exclusive means of redress and the case must be brought within two years of the violation. CISPA also prohibits using cyber threat indicators for regulatory purposes.	[neutral] CISPA would pre-empt any stronger state or local laws that have higher protections for privacy. CISPA would sunset without reauthorization after five years. While the sunset would provide an opportunity to debate the program's privacy impact and usefulness, debate would be limited without stronger transparency provisions about how the authority was used. The bill also exempts shared information from both federal and state freedom of information requirements. CISPA does not include a defensive measures provision.

	Safeguards for privacy and civil liberties	Preservation of long-standing, respective roles and	Provisions for appropriate sharing with targeted liability	Other considerations

		missions of civilian and intelligence agencies	protections	
National Cybersecurity Protection Advancement Act (NCPA) **Status:** Introduced in the House; Markup by House Homeland Security Committee	Grade: X In the National Cybersecurity Protection Advancement Act ("NCPA") "cyber threat indicator" is limited to information "necessary to describe or identify" certain things, including "any other attribute" of a cyber risk, though the attribute cannot be used to identify a specific person believed to be unrelated to the risk. Terms of service or licensing violations are explicitly excluded from the definition of cybersecurity risk. This information can be transmitted regardless of if sharing it would violate any other law. A second, separate provision further requires non-federal entities to take further reasonable efforts to remove information that can be used to identify specific persons and is reasonably believed to be unrelated to a cybersecurity risk or incident, as well as to safeguard that information from unauthorized access or acquisition. The bill requires the development and annual review of procedures governing "receipt, retention, use, and disclosure." The procedures are required to be consistent with Fair Information Practice Principles (FIPPS) as developed by DHS under the Privacy Act of 1974 (though other bills use another formulation of the FIPPS that is more robust). The procedures must be released publicly. The NCPAA also provides for a privacy and civil liberties report from the Comptroller General on the National Cybersecurity and Communications Integration Center (NCCIC) and comprehensive oversight reports from the Inspector General and DHS' Privacy and Civil Liberties Officer, in consultation with the Privacy and Civil Liberties Oversight Board, to oversee the implementation of the policies and procedures.	X The NCPA requires DHS to share information using a "rapid automated" process with the relevant "Sector Specific Agency," which can include the Department of Defense, and therefore the NSA, among other agencies. Once sent to the government, information can only be used for "cybersecurity purposes," not for other crimes. An approved amendment contains a prohibition on using the law against targeting a person for "surveillance," or for tracking an individual's personally identifiable information.	X The NCPA provides liability protection for entities, unless there is clear and convincing proof that the entity violated the law by way of "willful misconduct." The bill contains a private right of action against federal departments or agencies that either intentionally or willfully injure an individual in violation of the law. However, the provision has a two year statute of limitations from the date of the violation, notwithstanding when the injured individual finds out about the action. Additionally, an injury may be hard to ascertain, particularly since injuries are typically keyed to financial harm and significant privacy violations may not always have a financial component. The Chief Privacy Officer is responsible for, among other things, ensuring that there are sanctions in place for federal employees or agents who knowingly or willfully act in an unauthorized manner under the law and notifying certain entities, including Congressional committees but not the public, of significant violations.	X The NCPA would sunset without reauthorization after seven years. Notwithstanding that it may violate any other law, defensive measures may be used or shared under the NCPA, though not if a measure "destroys, renders unusable, or substantially harms" others' information systems. However, the provision allows for the use of defensive measures that may significantly, though not "substantially" harm another user or system. It does not limit effects of defensive measures to one's own network. The bill increases the role of the NCCIC, a government entity, to not only act as a gateway for cyber threat indicators domestically, but to engage with international partners on cyber threat indicators, though without providing for adequate transparency on the international exchange of information. The bill also exempts shared information from both federal and state freedom of information requirements. In an amendment process, the bill saw a number of changes likely to have a positive security impact: it would order the creation of best practices for coordinating vulnerability disclosures, create a comprehensive cybersecurity awareness campaign with input from across sectors, make self-assessment tools available to small and medium-sized businesses, and permit consultation with the National Institute of Standards and Technology -- an agency developed to coordinate the development of standards -- for the privacy and civil liberties policies and procedures. A new provision orders the DHS to assess the technical capacities of the United States and Industrial Control Systems Cyber Emergency Response Teams (CERTs). However, it doesn't specify whether or how DHS would exert control over the CERTs.

	Safeguards for privacy and civil liberties	Preservation of long-standing, respective roles and missions of	Provisions for appropriate sharing with targeted liability	Other considerations

		civilian and intelligence agencies	protections	
Protecting Cyber Networks Act (PCNA) **Citation:** H.R. 1560 **Status:** Introduced in the House; Marked up by House Intelligence Committee **URL** https://www.congress.gov/bill/114th-congress/house-bill/1560/all-actions-with-amendments/	Grade: X While the Protecting Cyber Networks Act's ("PCNA") definition of "cyber threat indicator" requires that information is necessary to describe or identify a cyber threat, it contains a catch-all provision similar to that in CISA that expands the definition of "cyber threat indicator" to cover "any other attributes of a cybersecurity threat, though only if disclosure of such attribute is not otherwise prohibited by law" and not protected by the First Amendment to the Constitution. Terms of service or licensing violations are explicitly excluded from the definition. This information could be shared with the government even if doing so would violate another law. Security controls must be created to prevent unauthorized access to information received by government. The PCNA requires entities to take "reasonable efforts" to remove information, or use a technical capability to do so, that would identify specific persons and is unrelated to the cybersecurity risk, but only if the entity knows about the information at the time of the sharing. The Attorney General would, in consultation with other federal agencies, establish privacy and civil liberties guidelines regarding the receipt, retention, use, and dissemination of cyber threat indicators. These guidelines would have to be consistent with the Fair Information Practice Principles (FIPPs) as set out in the National Strategy for Trusted Identities in Cyberspace, one of the most robust formulations of FIPPS. The bill would require separate biannual reports from the Director of National Intelligence and the Privacy and Civil Liberties Oversight Board, and relevant Inspector Generals, to include analyses of the privacy and civil liberties impact of the program. The Inspector General and National Intelligence reports could each have a classified annex. The PCNA also provides a report from the Comptroller General on efforts by the federal government to remove personal information.	X Unlike any other proposal, the PCNA would give primary control of coordinating cybersecurity information sharing to the "Cyber Threat Intelligence Integration Center," located within the Office of the Director of National Intelligence and operated from a building owned by the intelligence community. This would inappropriately undermine civilian control over domestic cybersecurity efforts and harm public transparency. The new Center would further ensure that information was shared in real time with "all of the appropriate Federal entities," including the Department of Defense. However, the PCNA does limit direct sharing with the Department of Defense and the National Security Agency. The PCNA would permit law enforcement to use cyber threat indicators to investigate a variety of crimes unrelated to cybersecurity. The Act does contain a prohibition on using the law against targeting a person for "surveillance," though the term is undefined.	X The PCNA provides broad liability protection to companies that, in good faith, transmit information (or fail to act on shared information) unless there is clear and convincing evidence that the company acted with "willful misconduct." The bill provides a remedy against a government agency that intentionally or willfully violates the mandated Attorney General's privacy and civil liberties guidelines to injure an individual. However, the provision has a two-year statute of limitations from the date of the violation, notwithstanding when the injured individual finds out about the action. Additionally, an injury may be hard to ascertain, particularly since injuries are typically keyed to financial harm and significant privacy violations may not always have a financial component. The President must establish, and submit to Congress, guidelines that ensure the existence of an audit capability and appropriate sanctions for employees or agents that knowingly or willfully act in violation of the bill.	X The PCNA would sunset without reauthorization after seven years. The PCNA allows the use of defensive measures, though it prohibits the "intentional or reckless" use of defensive measures that destroy or make unusable, among other harms, others' information systems. The language still broadly allows the use defensive measures, which negligently or unintentionally harms a large number of systems, effects that are highly plausible. The bill also exempts shared information from both federal and state freedom of information requirements.