ONE PAGE SUMMARY COMPARISON CHART: Information Sharing Authorities and Privacy Protections Under CISA, PCNA, and NCPAA

	Cybersecurity Act of 2015 (H.R. 2029, Division N)	Cybersecurity Information Sharing Act (CISA, S. 754)	Protecting Cyber Networks Act (PCNA, H.R. 1560 Title I)	National Cybersecurity Protection Advancement Act (H.R. 1731)
Definition of Cyber Threat Indicators	Includes provisions to share information that describes attributes and potential harms which may allow sharing of unnecessary PII or content. (adopted from CISA) **WORST**	Same as Cybersecurity Act of 2015. **WORST**	Same as Cybersecurity Act of 2015 and CISA. **WORST**	Includes provisions to share information that describes potential harms, when sharing information that describes attributes, sharing of PII is excluded. **INTERMEDIATE**
Sharing with Government	Direct sharing with any federal entity, including NSA. Liability protection for sharing through FBI/DNI portals upon President's certification. **WORST**	Direct sharing with any federal entity, including NSA. **VERY BAD**	Direct sharing with any federal entity, except DoD, which includes the NSA. **INTERMEDIATE**	Direct sharing only through DHS. **BEST**
Company Requirement to Remove Personal Information (PII)	Remove PII if you know it isn't directly related to threat. Creates a default that allows PII to be shared. **WORST**	Same as Cybersecurity Act of 2015. **WORST**	Remove PII if you reasonably believe it isn't directly related to threat. **BEST**	Remove PII if you reasonably believe it is unrelated to threat. **INTERMEDIATE**
Government Requirement to Remove PII before dissemination.	Timely destruction of PII if it's known it isn't directly related to threat. May be disseminated. (adopted from CISA) **WORST**	Same as Cybersecurity Act of 2015. **WORST**	Remove PII if government knows it is not directly related to a threat. NOTE: Contradicts dissemination requirement. **INTERMEDIATE**	Remove PII that DHS reasonably believes is unrelated to a cybersecurity threat. **BEST**
Liability Protection	Complete protection, including for gross negligence. No liability for inaction based on information received. **WORST**	Complete protection except in cases of gross negligence or willful misconduct. **INTERMEDIATE**	Complete protection except in cases of willful misconduct, includes failure to act. **VERY BAD**	Same as PCNA. **VERY BAD**
Sunset	10 years, with liability exception. (adopted from CISA). **WORST**	Same as Cybersecurity Act of 2015. **WORST**	7 years. **INTERMEDIATE**	Same as PCNA. **INTERMEDIATE**
Federal Law Enforcement Use Authorizations	Computer crimes; non-computer crimes like specific threats of terrorism, serious economic harm; ID theft, fraud, Espionage Act violations. **VERY BAD**	Computer crimes, and non-computer crimes like imminent threats of terrorism, serious economic harm; and ID theft, fraud, Espionage Act violations. **INTERMEDIATE**	Computer crimes, and non-computer crimes including serious violent felonies (no imminence); ID theft, fraud, Espionage Act violations. **WORST**	Cybersecurity purposes. **BEST**
Intra-Governmental Dissemination to DOJ/ FBI, DOD/NSA, etc.	Automatic dissemination unless unanimous consent for delay. (adopted from CISA) **INTERMEDIATE**	Same as Cybersecurity Act of 2015. **INTERMEDIATE**	Automatic dissemination, no delay or modification without cause. **WORST**	No mandatory dissemination requirement; DHS has discretion. **BEST**
Defensive Measures	Can't cause substantial harm or gain unauthorized access to another's system. (adopted from CISA) **BEST**	Same as Cybersecurity Act of 2015. **BEST**	Cannot cause substantial harm to another's information or system; limitation in authorization. **WORST**	Cannot cause substantial harm to another's information or system; limitation in definition. **INTERMEDIATE**

For more information, contact Robyn Greene, Policy Counsel, at greene@opentechinstitute.org.