# The Protecting Cyber Networks Act: Section-By-Section Analysis

*Section 1: Short Title; Table of Contents.*

The short title of the Act is the Protecting Cyber Networks Act.

*Section 2: Sharing of Cyber Threat Indicators and Defensive Measures by the Federal Government with Non-Federal Entities.*

This section of the Act amends Title I of the National Security Act by adding a new section, Section 111. Under this new section, the Director of National Intelligence, in consultation with the heads of the Departments of Homeland Security, Treasury, Justice, Commerce, and Defense (hereinafter the "appropriate Federal entities"), should create procedures to facilitate and promote the timely sharing of cyber threat indicators with the private sector. The procedures would promote the sharing of: classified cyber threat indicators with representatives of the private sector with appropriate security clearances; classified cyber threat indicators that may be declassified and shared at an unclassified level; and any information in the possession of the Federal Government about imminent or ongoing cyber threats that may allow private companies to prevent or mitigate those threats.

The procedures must also ensure the Federal Government creates and maintains the capability to share cyber threat indicators in real time with the private sector, consistent with the protection of classified information.

Additionally, the procedures drafted by the Director of National Intelligence will require federal agencies to perform a review of cyber threat indicators they receive from the private sector before the agencies share those indicators within the Federal Government. In that review, the receiving agencies will assess whether—despite the private sector's own requirement to conduct a similar review—the cyber threat indicators contain any personal information or information identifying a specific person that does not directly relate to a cyber threat. If so, the Federal Government must remove that information. The Federal Government must implement a technical capability configured to remove the information.

*Section 3: Authorizations for Preventing, Detecting, Analyzing, and Mitigating Cybersecurity Threats.*

Subsection (a) of this section authorizes private entities to engage in defensive monitoring of their own networks and the networks of non-Federal entities that have consented to monitoring. Subsection (a) does not authorize the Federal Government to conduct surveillance of any person.

Subsection (b) of this section authorizes private entities to operate defensive measures on their own networks and the networks of non-Federal entities that have consented to the operation of defensive measures. Subsection (b) does not authorize non-Federal entities to intentionally or recklessly operate any defensive measure that destroys, render unusable or inaccessible (in whole or in part), substantially harms, or initiates a new action, process, or procedure on any network that does not belong to them or to a non-Federal entity that has not consented to the operation of those defensive measures. As a result, subsection (b) does not authorize "hacking back" or any other form of cyber operation that takes place on computers or networks without the consent of the owner of those computers or networks.

Subsection (c) of this section authorizes non-Federal entities, notwithstanding any other provision of law, to share or receive cyber threat indicators or defensive measures for cybersecurity purposes with other non-Federal entities. This subsection also authorizes non-Federal entities to share or receive cyber threat indicators or defensive measures with appropriate Federal entities other than the Department of Defense and the National Security Agency. Even so, subsection (c) expressly states that companies may share cyber threat information or defensive measures with the Department of Defense and the National Security Agency if they are authorized to do so by another applicable law or regulation.

Before sharing, non-Federal entities must, under the requirements of subsection (d), take reasonable efforts to review cyber threat indicators and defensive measures for any personal information or information identifying a specific person that does not directly relate to a cyber threat. If cyber threat indicators or defensive measures contain that kind of information, non-Federal entities must take reasonable efforts to remove the information before sharing. Subsection (d) also permits non-Federal entities to use cyber threat indicators and defensive measures to monitor or operate defensive measures on their own networks and the networks of other non-Federal entities that have consented to the operation of the defensive measures.

In addition, subsection (d) permits state and local governments to use cyber threat indicators for certain law enforcement purposes; the subsection also exempts those shared cyber threat indicators from state and local disclosure laws.

*Section 4: Sharing of Cyber Threat Indicators and Defensive Measures with Appropriate Federal Entities Other than the Department of Defense or the National Security Agency.*

Subsection (a) of this section amends Title I of the National Security Act of 1947, as amended by Section 2 of the Act, to add a subsection (b) to the newly created Section 111. The new subsection requires the President to develop and submit to Congress policies and procedures for the receipt of cyber threat indicators and defensive measures by the Federal Government. Those policies and procedures must ensure that, when an appropriate federal entity other than the Department of Defense or the National Security Agency receives a cyber threat indicator under Section 3 of the Act, that federal entity shares the cyber threat indicator in real time with all other appropriate Federal entities, including all relevant components of those other appropriate federal entities. Among other things, the procedures must also ensure that additional Federal entities beyond the appropriate Federal entities receive cyber threat indicators when those indicators are relevant.

Subsection (b) of this section requires the Attorney General, in consultation with the heads of other appropriate federal entities, to develop and periodically review privacy and civil liberties guidelines. The Attorney General guidelines will govern the receipt, retention, use, and dissemination of cyber threat indicators obtained by the Federal Government under the Act. The guidelines must also establish, among other things: a process for the prompt destruction of any personal information or information identifying a specific person that does not directly relate to a cyber threat; specific limitations on the length of time for which a cyber threat indicator can be retained; and a process to inform recipients of cyber threat indicators that the indicators may only be used for cybersecurity purposes. The Attorney General must submit an interim version of the guidelines to Congress within 90 days of the enactment of the Act, and a final version within 180 days.

Subsection (c) of this section further amends Title I of the National Security Act of 1947 by inserting a new Section 119B. That new section establishes the Cyber Threat Intelligence Integration Center (CTIIC) within the Office of the Director of National Intelligence. Section 119B also lays out the missions of the CTIIC and imposes certain limitations regarding the center's personnel and location.

Subsection (d) of this section states that the act of sharing a cyber threat indicator with the Federal Government does not constitute a waiver of any applicable privilege or protection provided by law. The subsection also establishes that cyber threat indicators shared with the Federal Government remain the proprietary information of the sharing non-Federal entity, are exempt from federal disclosure laws, and do not constitute ex parte communications in a judicial or regulatory proceeding.

Additionally, subsection (d) lays out the purposes for which the Federal Government may use a cyber threat indicator it receives from a non-Federal entity under the Act. The Federal Government may use shared cyber threat indicators solely for: a cybersecurity purpose; preventing or prosecuting a threat of death or seriously bodily harm or an offense arising out such a threat; preventing or prosecuting a serious threat to a minor, including sexual exploitation; or preventing or prosecuting espionage, economic espionage, serious violent felonies, and violations of the Computer Fraud and Abuse Act.

*Section 5: Federal Government Liability for Violations of Privacy and Civil Liberties*.

Section 5 creates a private cause of action against the Federal Government if a department or agency intentionally or willfully violates the privacy and civil liberties guidelines issued by the Attorney General under Section 4(b) of the Act. The section also establishes statutory damages for a violation of the Attorney General guidelines, provides for reasonable attorney fees for injured persons, specifies the possible venues for an action, and creates a statute of limitations for the new cause of action. Lastly, Section 5 clarifies that this cause of action is the exclusive means available to a complainant seeking a remedy for a violation of the Act by a department or agency of the Federal Government.

*Section 6: Protection from Liability.*

This section states that no cause of action shall lie or be maintained in any court against any private entity acting in good faith for the monitoring of an information system or information under Section 3(a) of the Act or for the sharing or receipt of cyber threat indicators or defensive measures under Section 3(c) of the Act. Nothing in Section 6, however, shall be construed to require the dismissal of a cause of action against a non-Federal entity that has engaged in willful misconduct in the course of conducting activities authorized by the Act. Section 6 also defines the term "willful misconduct" for the purposes of the section and establishes the standard by which a plaintiff may prove willful misconduct.

*Section 7: Oversight of Government Activities.*

Subsection (a) of this section further amends Section 111 of the National Security Act of 1947, as created by the Act, to require a biennial report by the Director of National Intelligence, in consultation with the heads of other appropriate Federal entities, on the implementation of the Act.

Subsection (b) of this section requires two reports on privacy liberties. First, subsection (b) requires the Privacy and Civil Liberties Oversight Board to submit to Congress a biennial

report on the privacy and civil liberties impact of the Act. Second, subsection (b) requires the Inspectors General of certain appropriate Federal entities, in consultation with the Council of Inspectors General on Financial Oversight, to jointly submit a biennial report to Congress on the receipt, use, and dissemination of cyber threat indicators shared with the Federal Government under the Act.

*Section 8: Report on Cybersecurity Threats.*

This section requires the Director of National Intelligence, in consultation with the heads of appropriate elements of the Intelligence Community, to submit a report to the congressional intelligence committees on cybersecurity threats, including cyber attacks, theft, and data breaches. The report shall be submitted in unclassified form, but may contain a classified annex.

*Section 9: Construction and Preemption*.

Section 9 contains a variety of construction and preemption provisions to clarify the scope of the Act. Among other things, these provisions make clear that nothing in the Act authorizes the Department of Defense or any element of the Intelligence Community, including the National Security Agency, to target a person for surveillance. The provisions also state that nothing in the Act shall be construed to limit or modify any existing information-sharing relationships outside of the Act or prohibit any new information-sharing relationships outside of the Act; the legislation also supersedes any provision of state or local law that may restrict or otherwise expressly regulate an activity authorized under the Act.

*Section 10: Conforming Amendments*.

This section contains conforming amendments to Section 552(b) of title 5, United States Code.

*Section 11: Definitions*.

Section 11 provides definitions for a number of key terms used in the Act. These definitions—in particular, the definitions of the terms "cybersecurity purpose," "cyber threat," "cyber threat indicator," and "defensive measure"—narrowly cabin the scope and breadth of the Act.