

# **H.R. 1731: The Nation Cybersecurity Protection Advancement Act of 2015**

## **Section by Section**

### **Section 1. Short Title.**

This section provides that the bill may be cited as the “National Cybersecurity Protection Advancement Act of 2015.”

### **Section 2. National Cybersecurity and Communications Integration Center.**

This section amends subsection (a) of the second section 226 (6 U.S. Code 148) of the Homeland Security Act of 2002 by adding definitions of terms used in the bill, including: “cyber threat indicator”, “cybersecurity purpose”, “defensive measure”, “network awareness”, “private entity”, “security control”, and “sharing”.

### **Section 3. Information Sharing Structure and Process.**

This section amends subsection (a) of the second section 226 of the Homeland Security Act of 2002 as described below.

#### ***Amendments to the National Cybersecurity and Communications Integration Center.***

This section amends the functions of the NCCIC. It designates the NCCIC as the “lead Federal civilian interface” for multi-directional and cross-sector information sharing related to cybersecurity.

It also adds cyber threat indicators and defensive measures to the types of technical threat data that the NCCIC will collect, analyze, and share to provide enhanced situational awareness to Federal, non-Federal and private entities. It directs the NCCIC to share information relating to cybersecurity risks and incidents with small and medium-sized businesses, as appropriate.

It directs the NCCIC to promptly notify the Secretary of Homeland Security (the Secretary) and Congress of any significant violations of information sharing policies and procedures, and promptly notify non-Federal entities that have shared information that is known or determined to be in error. As the lead civilian interface for sharing cyber threat information with the Government, the NCCIC is uniquely positioned as a sharing hub to integrate information from multiple sources, and use the information to Government Agencies and the private sector with actionable information to recognize and stop attacks before harm is done.

This section directs the NCCIC to engage with international partners on cybersecurity, and expands the composition of the NCCIC to include an entity to collaborate with state and local governments; the U.S. Computer Emergency Readiness Team to coordinate information related to cybersecurity risks and incidents and provide technical assistance; the Industrial Control System Cyber Emergency Response Team to coordinate with industrial control systems owners

and operators; and the National Coordinating Center for Communications to coordinate the resilience and recovery of national security emergency communications.

H.R. 1731 amends second section 226, the provisions of which are described below:

**(g) Rapid Automated Sharing.**

This subsection requires the Under Secretary for Cybersecurity and Infrastructure Protection, in coordination with industry and other stakeholders, to develop an automated capability for the timely sharing of cyber threat indicators and defensive measures. It also directs the NCCIC to develop the capability to share cyber threat indicators and defensive measures with each Federal Agency designated as the ‘Sector Specific Agency’ (SSA) for each critical infrastructure sector in as close to real time as practicable. It directs the Under Secretary for Cybersecurity and Infrastructure Protection to submit a biannual report to the appropriate congressional committees on the progress of developing this capability.

**(h) Sector Specific Agencies**

This subsection directs the Secretary to recognize the SSA for each critical infrastructure sector based on the Department’s National Infrastructure Protection Plan as of March 25, 2015. It directs the Secretary, in coordination with the heads of each SSA, to support the security and resilience activities of the specific sectors, provide institutional knowledge and expertise, and support timely sharing of information.

**(i) Voluntary Information Sharing Procedures**

Subsection (i) outlines the information sharing procedures and permits the NCCIC to enter into voluntary information sharing relationships with any consenting non-Federal entity for the sharing of cyber threat indicators and defensive measures for cybersecurity purposes. To prevent personal information from inadvertently being shared, the non-Federal entity sharing the information is required to remove all personal information unrelated to the cybersecurity risk before sharing with the NCCIC or other non-Federal entities. This subsection outlines the information sharing agreements, authorizations, civil liberty and information protections, and antitrust exemption of these relationships.

**(2) Agreements**

Subsection (i)(2) allows the Center to utilize standard and negotiated agreements as the types of agreements that non-Federal entities may enter into with the NCCIC for the purposes of this Act. However, it makes clear that agreements are not limited to just these types, and pre-existing agreements between the NCCIC and the non-Federal entity will be in compliance with this section.

**(3) Information Sharing Authorization**

Subsection (i)(3) authorizes a non-Federal entity to share cyber threat indicators or defensive measures obtained from its own information system or, with written consent, from an information system of another Federal or non-Federal entity, with another non-Federal entity and the NCCIC for cybersecurity purposes. It requires that recipients of this information comply with lawful restrictions on sharing or use. It also requires a recipient of information from another Federal or non-Federal entity to comply with lawful restrictions placed on the information by the sharing Federal or non-Federal entity.

This subsection also requires the Under Secretary for Cybersecurity and Infrastructure Protection, in coordination with industry and other stakeholders to develop and adhere to policies and procedures for coordinating vulnerability disclosures, to the extent practicable, with international standards in the information technology industry.

This subsection also requires a non-Federal entity to take reasonable efforts to remove information that could be used to identify specific persons reasonably believed at the time of sharing to be unrelated to a cybersecurity threat, and safeguard information that can be used to identify specific persons from unintended disclosure and unauthorized access or acquisition.

#### **(4) Network Awareness Authorization**

Subsection (i)(4) authorizes a non-Federal entity, not including a State, local, or Tribal government, to conduct network awareness of its own information system, or the information system of another non-Federal or Federal entity with written consent, for cybersecurity purposes.

#### **(5) Defensive Measure Authorization**

Subsection (i)(5) authorizes a non-Federal entity, not including a State, local, or Tribal government, to conduct network awareness defensive measure that is applied only to its own information system, or the information system of another non-Federal or Federal entity with written consent, for cybersecurity purposes.

#### **(6) Privacy and Civil Liberties Protections**

Subsection (i)(6) requires the Under Secretary in coordination with the Chief Privacy Officer and the Officer for Civil Rights and Civil Liberties at the Department to establish and annually review policies and procedures for the Department that govern the receipt, retention, use, and disclosure of cyber threat indicators and information related to cybersecurity risks and incidents.

This subsection requires that certain policies and procedures to minimize any impact on privacy and civil liberties should be established consistent with the need to protect information systems from, and conduct mitigation of, cybersecurity risks and incidents in a timely manner.

The subsection requires the Chief Privacy Officer to submit a report to the appropriate congressional committees, no later than 180 days after enactment of this Act, that describes the policies and procedures governing the sharing of cyber threat indicators and defensive measures. The subsection also requires the Chief Privacy Officer to monitor the implementation of these

policies and procedures, and regularly review and update privacy impact assessments to ensure all relevant constitutional, legal, and privacy protections are being followed. The subsection further requires the Chief Privacy Officer to submit an annual report to Congress on the effectiveness of these policies and procedures, ensuring appropriate sanctions are in place for employees, agents, and contractors of the Department who intentionally or willfully conduct unauthorized activities under this section.

Additionally, the subsection requires the Undersecretary to ensure that a public notice is made of the policies and procedures governing the sharing of cyber threat indicators and defensive measures.

This subsection requires the Department's Office of the Inspector General (DHS OIG) to submit a report to Congress within two years of enactment of this Act and periodically thereafter that includes a review of the type of information shared with NCCIC, the use of any information and actions taken by NCCIC, and the impact, if any, of sharing of such information on privacy and civil liberties.

This subsection requires that the Department's Chief Privacy Officer and Officer for Civil Rights and Civil Liberties also submit a report to Congress within two years of enactment of this Act that assesses the impact on privacy and civil liberties of the information sharing activities under this section. The report shall include appropriate recommendations to minimize or mitigate the impact of the sharing of cyber threat indicators and defensive measures under this section.

### **(7) Uses and Protection of Information**

This subsection sets forth the roles and responsibilities for non-Federal entities, Federal entities, and State, Tribal, and local governments for using and protecting information shared through the NCCIC or otherwise.

#### ***Non-Federal Entities***

Subsection (i)(7) permits a non-Federal entity that shares cybersecurity information with the NCCIC, or another non-Federal entity, to use, retain, or disclose those cyber threat indicators and defensive measures solely for cybersecurity purposes. It requires non-Federal entities to remove information that could be used to identify specific persons reasonably believed at the time of sharing to be unrelated to a cybersecurity threat and safeguard information that can be used to identify specific persons prior to sharing the information. Non-Federal entities must comply with appropriate restrictions placed on the subsequent disclosure or retention of cyber threat indicators or defensive measures by a Federal or non-Federal entity. This subsection further stipulates that information shared with the NCCIC will be deemed to have been voluntarily shared. This subsection requires that a non-Federal entity implements and utilizes a security control to protect against unauthorized access to or acquisition of cyber threat indicators or defensive measures, and it prohibits the use of such cyber security information to gain an unfair or competitive advantage over any non-Federal entity.

#### ***Federal Entities***

This subsection permits Federal entities that receive cyber threat indicators or defensive measures to use, retain, or further disclose this information solely for cybersecurity purposes. This subsection requires Federal entities to take reasonable to efforts to remove information that could be used to identify specific persons reasonably believed at the time of sharing to be unrelated to a cybersecurity threat and safeguard information that can be used to identify specific persons prior to sharing the information. This subsection further stipulates that information shared with the NCCIC will be deemed to have been voluntarily shared. This subsection requires that a Federal entity implements and utilizes a security control to protect against unauthorized access to or acquisition of cyber threat indicators or defensive measures.

The cybersecurity information is exempt from disclosure under the Freedom of Information Act (FOIA), 5 U.S. Code 552, or non-Federal disclosure laws and withheld, without discretion, from the public under 5 U.S. Code 552(3)B). This subsection allows a Federal or non-Federal entity to designate information shared with the Center as commercial, financial, and proprietary information. The information shared is prohibited from being used for regulatory purposes, and may not constitute a waiver of applicable privileges or protections provided by law, including trade secret protections. The information is also not subject to judicial doctrine or rules of federal entities regarding ex parte communications.

#### ***State, Tribal, or Local Government***

This subsection permits State, Tribal or local governments that receive cyber threat indicators or defensive measures to use, retain, or further disclose this information solely for cybersecurity purposes. It requires prior to sharing that reasonable efforts be made to remove information that could be used to identify specific persons reasonably believed to be unrelated to a cybersecurity threat and safeguard information that can be used to identify specific persons prior to sharing the information. This subsection allows a Federal or non-Federal entity to designate information shared with the Center as commercial, financial, and proprietary information. This subsection further stipulates that information shared with the NCCIC will be deemed to have been voluntarily shared. This subsection requires that a State, Tribal or local government implement and utilize security controls to protect against unauthorized access to or acquisition of cyber threat indicators or defensive measures. This subsection states that cybersecurity information is exempt from disclosure under State, Tribal or local disclosure laws, and may not be used to regulate the lawful activity of a non-Federal entity.

#### **(8) Liability Exemptions**

Subsection (i)(8) provides that no cause of action shall lie or be maintained in any court, and such action shall be promptly dismissed, against any non-Federal entity that conducts network awareness or shares cyber threat indicators or defensive measures, for cybersecurity purposes, in accordance with paragraphs (4) and (3), respectively, and the other provisions in section 3 of the bill. This subsection also provides liability protection for a non-Federal entity that fails to act upon shared cyber threat indicators or defensive measures.

However, non-Federal entities do not receive liability protection for egregious actions that rise to the level of willful misconduct. Willful misconduct is defined in the subsection as an act or omission that is taken intentionally to achieve a wrongful purpose, knowingly without legal or factual justification, and in disregard of a known or obvious risk that is so great as to make it highly probable that the harm will outweigh the benefit. If a plaintiff files suit claiming willful misconduct by a non-Federal entity, the plaintiff must prove willful misconduct by clear and convincing evidence and establish that the non-Federal entity's willful misconduct proximately caused the plaintiff's injury.

#### **(9) Federal Government Liability for Violations of Restrictions on the Use and Protection of Voluntarily Shared Information**

Subsection (i)(9) provides a clear path for injured persons to sue a Federal government department or agency for an intentional or willful violation of the uses and protections of voluntarily shared cyber threat indicators, defensive measures, or cybersecurity information as laid out in subsections (i)(3), (i)(6), and (i)(7)(B), and any other applicable provisions of section 3. This subsection further provides for statutory damages for such a violation, venue selection for an action under this provision, and the statute of limitations for bringing such an action.

#### **(10) Antitrust Exemption**

This subsection exempts non-Federal entities from violations of U.S. antitrust law for sharing cybersecurity information, or providing assistance for cybersecurity purposes, provided that the action is taken to assist with preventing, investigating, or mitigating a cybersecurity risk or incident. This subsection makes it clear that the exemption cannot be utilized for monopolistic activities such as price-fixing, or sharing of price or cost information, customer lists, or information regarding future planning.

#### **(11) Construction and Preemption**

Subsection (i)(11) contains a number of construction and preemption provisions that address the scope of the Act. Specifically, the provisions address otherwise lawful disclosures and preserve whistleblower protections. Nothing in the Act should be construed to affect any requirements under other provisions of law for non-Federal entities providing information to Federal entities. The provisions preserve existing contractual obligations and rights. They also prohibit the Federal government from requiring non-Federal entities to provide it with cybersecurity related information as a condition for the award of a grant, contract or purchase agreement. This subsection reiterates that any sharing of cybersecurity information under this legislation is purely voluntary, and that non-Federal entities are not subject to liability for choosing not to engage in such voluntary information sharing activities. This subsection also does not authorize or modify any existing Federal authority to retain and use cybersecurity information shared under the bill for purposes other than those permitted in this Act. This legislation also supersedes any provision of state or local law that may restrict or otherwise expressly regulate an activity authorized under this Act.

### **Section 4. Information Sharing and Analysis Organizations.**

This section amends Section 212 of the Homeland Security Act to broaden the functions of Information Sharing and Analysis Organizations (ISAOs) to include cybersecurity risk and incident information beyond that pertaining to critical infrastructure. This section also adds references to the definitions of ‘cybersecurity risk’ and ‘incident’ as they relate to the NCCIC in the second section 226 of the Homeland Security Act.

#### **Section 5. Streamlining of Department of Homeland Security Cybersecurity and Infrastructure Protection Organization.**

This section renames The National Protection and Programs Directorate of the Department of Homeland Security, the “Cybersecurity and Infrastructure Protection Directorate”. It requires the Secretary to submit a report to Congress on the feasibility of making the Cybersecurity and Communications Office an operational component of the Department.

Nothing in this section should be construed to alter the mission or reporting structure of the Office of Emergency Communications. Pursuant to 6 U.S.C. 571, the Director of the Office of Emergency Communications reports to the Assistant Secretary for Cybersecurity and Communications. The Department shall submit any proposed changes to this reporting structure to the Committee for review and approval.

#### **Section 6. Cyber Incident Response Plans.**

This section requires the Secretary, in coordination with the heads of other Federal departments and agencies to update, maintain, and exercise the Cyber Incident Annex to the National Response Framework of the Department.

#### **Section 7. Security and Resiliency of Public Safety Communications; Cybersecurity Awareness Campaign.**

This section requires the NCCIC, in coordination with the Office of Emergency Communications, to assess the effects of cyber incidents on public safety communications.

This section also requires the Under Secretary for Cybersecurity and Infrastructure Protection to develop and implement a cybersecurity awareness campaign regarding cybersecurity risks and voluntary best practices for mitigating and responding to cybersecurity risks.

#### **Section 8. Critical Infrastructure Protection Research and Development.**

This section requires the Secretary, acting through the Under Secretary for Science and Technology, to submit a strategic plan to Congress within 180 days for guiding the direction of Federal physical security and cybersecurity technology research and development efforts for protecting critical infrastructure against all threats.

#### **Section 9. Report on Reducing Cybersecurity Risks in DHS Data Centers.**

This section requires the Secretary to submit a report to Congress on the feasibility of the Department creating an environment for the reduction of cybersecurity risks at the Department's data centers.

**Section 10. Assessment.**

This section requires the Comptroller General of the United States to submit a report to Congress assessing the implementation of this Act no later than two years after the date of enactment of this Act.

**Section 11. Consultation.**

This section requires the Under Secretary for Cybersecurity and Infrastructure Protection to produce a report on the feasibility of creating a risk-informed plan should multiple critical infrastructure sectors experience cyber incidents simultaneously.

**Section 12. Technical Assistance.**

This section requires the Inspector General of the Department to review the operations of the United States Computer Emergency Readiness Team (US-CERT) and the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) to assess their capacity to provide technical assistance to non-Federal entities.

**Section 13. Prohibition on New Regulatory Authority.**

This section clarifies that nothing in this Act shall be construed to grant the Secretary any authority to promulgate regulations or set standards relating to the cybersecurity of non-Federal entities, not including State, local, or Tribal governments.

**Section 14. Sunset.**

This section requires that any reporting requirements required by this Act terminate seven years after the date of enactment of this Act.

**Section 15. Prohibition on New Funding.**

This section states that no new funds are authorized to be appropriated to carry out this Act.