JOINT EXPLANATORY STATEMENT TO ACCOMPANY THE CYBERSECURITY ACT OF 2015

The following consists of the joint explanatory statement to accompany the Cybersecurity Act of 2015.

This joint explanatory statement reflects the status of negotiations and disposition of issues reached between the Senate Select Committee on Intelligence, the House Permanent Select Committee on Intelligence, the Senate Committee on Homeland Security and Governmental Affairs, and the House Committee on Homeland Security. The joint explanatory statement shall have the same effect with respect to the implementation of this Act as if it were a joint explanatory statement of a committee of conference.

The joint explanatory statement comprises an overview of the bill's background and objectives, and a section-by-section analysis of the legislative text.

PART I: BACKGROUND AND NEED FOR LEGISLATION

Cybersecurity threats continue to affect our nation's security and its economy, as losses to consumers, businesses, and the government from cyber attacks, penetrations, and disruptions total billions of dollars. This legislation is designed to create a *voluntary* cybersecurity information sharing process that will encourage public and private sector entities to share cyber threat information, without legal barriers and the threat of unfounded litigation—while protecting private information. This in turn should foster greater cooperation and collaboration in the face of growing cybersecurity threats to national and economic security.

This legislation also includes provisions to improve Federal network and information system security, provide assessments on the Federal cybersecurity workforce, and provide reporting and strategies on cybersecurity industry-related and criminal-related matters. The increased information sharing enabled by this bill is a critical step toward improving cybersecurity in America.

PART II: SECTION-BY-SECTION ANALYSIS AND EXPLANATION OF LEGISLATIVE TEXT

The following is a section-by-section analysis and explanation of the Cybersecurity Act of 2015.

TITLE I–CYBERSECURITY INFORMATION SHARING

Section 101. Short title.

Section 101 states that Title I may be cited as the "Cybersecurity Information Sharing Act of 2015."

Section 102. Definitions.

Section 102 defines for purposes of this title key terms such as "cybersecurity purpose," "cybersecurity threat," "cyber threat indicator," "defensive measure," and "monitor." The definition of "cybersecurity purpose" is meant to include a broad range of activities taken to protect information and information systems from cybersecurity threats. The authorizations under this Act are tied to conduct undertaken for a "cybersecurity purpose," which both clarifies their scope and ensures that the authorizations cover activities that can be performed in conjunction with one another. For instance, a private entity conducting monitoring activities to determine whether it should use an authorized "defensive measure" would be monitoring for a "cybersecurity purpose." Significantly, the authorization for "defensive measures" does not include activities that are generally considered "offensive" in nature, such as unauthorized access of, or execution of computer code on, another entity's information systems, such as "hacking back" activities, or any actions that would substantially harm another private entity's information systems, such as violations of section 1030, of title 18, United States Code.

Section 103. Sharing of information by the Federal Government.

Section 103 requires the Director of National Intelligence, the Secretary of Homeland Security, the Secretary of Defense, and the Attorney General to jointly develop and issue procedures for the timely sharing of classified and unclassified cyber threat indicators and defensive measures (hereinafter referenced collectively in this joint explanatory statement as, "cyber threat information") with relevant entities.

These procedures must also ensure the Federal Government maintains: a real-time sharing capability; a process for notifying entities that have received cyber threat information in error; protections against unauthorized access; and procedures to review and remove, prior to sharing cyber threat information, any information not directly related to a cybersecurity threat known at the time of sharing to be personal information of a specific individual or that identifies a specific individual, or to implement a technical capability to do the same. These procedures must be developed in consultation with appropriate Federal entities, including the Small Business Administration and the National Laboratories.

Section 104. Authorizations for preventing, detecting, analyzing, and mitigating cybersecurity threats.

Section 104 authorizes private entities to monitor their information systems, operate defensive measures, and share and receive cyber threat information. Private entities must, prior to sharing cyber threat information, review and remove any information not directly related to a cybersecurity threat known at the time of sharing to be personal information of a specific individual or that identifies a specific individual, or to implement and utilize a technical capability to do the same.

Section 104 permits non-Federal entities to use cyber threat information for cybersecurity purposes, to monitor, or to operate defensive measures on their information systems or on those of another entity (upon written consent). Cyber threat information shared by an entity with a

State, tribal, or local department or agency may be used for the purpose of preventing, investigating, or prosecuting any of the offenses described in Section 105, below. Cyber threat information is exempt from disclosure under any State, tribal, local, or freedom of information or similar law.

Section 104 further provides that two or more private entities are not in violation of antitrust laws for exchanging or providing cyber threat information, or for assisting with the prevention, investigation, or mitigation of a cybersecurity threat.

Section 105. Sharing of cyber threat indicators and defensive measures with the Federal Government.

Section 105 directs the Attorney General and Secretary of Homeland Security to jointly develop policies and procedures to govern how the Federal Government shares information about cyber threats, including via an automated real-time process that allows for information systems to exchange identified cyber threat information without manual efforts, subject to limited exceptions that must be agreed upon in advance. Section 105 also directs the Attorney General and Secretary of Homeland Security, in coordination with heads of appropriate Federal entities and in consultation with certain privacy officials and relevant private entities, to jointly issue and make publicly available final privacy and civil liberties guidelines for Federal entity-based cyber information sharing.

Section 105 directs the Secretary of Homeland Security, in coordination with heads of appropriate Federal entities, to develop, implement, and certify the capability and process through which the Federal Government receives cyber threat information shared by a non-Federal entity with the Federal Government. This section also provides the President with the authority to designate an appropriate Federal entity, other than the Department of Defense (including the National Security Agency), to develop and implement an additional capability and process following a certification and explanation to Congress, as described in this section. The capability and process at the Department of Homeland Security, or at any additional appropriate Federal entity designated by the President, does not prohibit otherwise lawful disclosures of information related to criminal activities, Federal investigations, or statutorily or contractually required disclosures. However, this section does not preclude the Department of Defense, including the National Security Agency from assisting in the development and implementation of a capability and process established consistent with this title. It also shall not be read to preclude any department or agency from requesting technical assistance or staffing a request for technical assistance.

Section 105 further provides that cyber threat information shared with the Federal Government does not waive any privilege or protection, may be deemed proprietary information by the originating entity, and is exempt from certain disclosure laws. Cyber threat information may be used by the Federal government for: cybersecurity purposes; identifying a cybersecurity threat or vulnerability; responding to, preventing, or mitigating a specific threat of death, a specific threat of serious bodily harm, or a specific threat of serious economic harm, including a terrorist act or a use of a weapon of mass destruction; responding to, investigating, prosecuting,

preventing, or mitigating a serious threat to a minor; or preventing, investigating, disrupting, or prosecuting an offense arising out of certain cyber-related criminal activities.

Finally, Section 105 provides that cyber threat information shared with the Federal Government shall not be used by any Federal, State, tribal, or local government to regulate non-Federal entities' lawful activities.

Section 106. Protection from liability.

Section 106 provides liability protection for private entities that monitor, share, or receive cyber threat information in accordance with Title I, notwithstanding any other provision of Federal, State, local, or tribal law. Section 106 further clarifies that nothing in Title I creates a duty to share cyber threat information or a duty to warn or act based on receiving cyber threat information. At the same time, nothing in Title I broadens, narrows, or otherwise affects any existing duties that might be imposed by other law; Title I also does not limit any common law or statutory defenses.

Section 107. Oversight of Government activities.

Section 107 requires reports and recommendations on implementation, compliance, and privacy assessments by agency heads, Inspectors General, and the Comptroller General of the United States, to ensure that cyber threat information is properly received, handled, and shared by the Federal Government.

Section 108. Construction and preemption.

Section 108 contains Title I construction provisions regarding lawful disclosures; whistleblower protections; protection of sources and methods; relationship to other laws; prohibited conduct, such as anti-competitive activities; information sharing relationships; preservation of contractual rights and obligations; anti-tasking restrictions, including conditions on cyber threat information sharing; information use and retention; Federal preemption of State laws that restrict or regulate Title I activities, excluding those concerning the use of authorized law enforcement practices and procedures; regulatory authorities; the Secretary of Defense's authorities to conduct certain cyber operations; and Constitutional protections in criminal prosecutions.

Section 109. Report on cybersecurity threats.

Section 109 requires the Director of National Intelligence, with the heads of other appropriate Intelligence Community elements, to submit a report to the congressional intelligence committees on cybersecurity threats, including cyber attacks, theft, and data breaches.

Section 110. Exception to limitation on authority of Secretary of Defense to disseminate certain information.

Section 110 clarifies that, notwithstanding Section 393(c)(3) of title 10, United States Code, the Secretary of Defense may authorize the sharing of cyber threat indicators and defensive measures pursuant to the policies, procedures, and guidelines developed or issued under this title.

Section 111. Effective period.

Section 111 establishes Title I and the amendments therein are effective during the period beginning on the date of enactment of this Act and ending on September 30, 2025. The provisions of Title I will remain in effect however, for action authorized by Title I or information obtained pursuant to action authorized by Title I, prior to September 30, 2025.

TITLE II–NATIONAL CYBERSECURITY ADVANCEMENT

SUBTITLE A – NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER

Section 201. Short title.

Section 201 establishes that Title II, Subtitle A may be cited as the "National Cybersecurity Protection Advancement Act of 2015".

Section 202. Definitions.

Section 202 defines for purposes of Title II, Subtitle A, the terms "appropriate congressional committees," "cybersecurity risk," "incident," "cyber threat indicator," "defensive measure," "Department," and "Secretary."

Section 203. Information sharing structure and processes.

Section 203 enhances the functions of the Department of Homeland Security's National Cybersecurity and Communications Integration Center, established in section 227 of the Homeland Security Act of 2002 (redesignated by this Act). It designates the Center as a Federal civilian interface for multi-directional and cross-sector information sharing related to cybersecurity risks, incidents, analysis and warnings for Federal and non-Federal entities, including the implementation of Title I of this Act. This section requires the Center to engage with international partners; conduct information sharing with Federal and non-Federal entities; participate in national exercises; and assess and evaluate consequence, vulnerability and threat information regarding cyber incidents to public safety communications. Additionally, this section requires the Center to collaborate with state and local governments on cybersecurity risks and incidents. The Center will comply with all policies, regulations, and laws that protect the privacy and civil liberties of United States persons, including by working with the Privacy Officer to ensure the Center follows the privacy policies and procedures established by title I of this Act.

Section 203 requires the Department of Homeland Security, in coordination with industry and other stakeholders, to develop an automated capability for the timely sharing of cyber threat indicators and defensive measures. It is critical for the Department to develop an automated system and supporting processes for the Center to disseminate cyber threat indicators and defensive measures in a timely manner.

This section permits the Center to enter into voluntary information sharing relationships with any consenting non-Federal entity for the sharing of cyber threat indicators, defensive measures, and information for cybersecurity purposes. This section is intended to provide the Department of Homeland Security additional options to enter into streamlined voluntary information sharing agreements. This section allows the Center to utilize standard and negotiated agreements as the types of agreements that non-Federal entities may enter into with the Center. However, it makes clear that agreements are not limited to just these types, and pre-existing agreements between the Center and the non-Federal entity will be in compliance with this section.

Section 203 requires the Director of the Center to report directly to the Secretary for significant cybersecurity risks and incidents. This section requires the Secretary to submit to Congress a report on the range of efforts underway to bolster cybersecurity collaboration with international partners. Section 203 allows the Secretary to develop and adhere to Department policies and procedures for coordinating vulnerability disclosures.

Section 204. Information sharing and analysis organizations.

Section 204 amends Section 212 of the Homeland Security Act to clarify the functions of Information Sharing and Analysis Organizations (ISAOs) to include cybersecurity risk and incident information beyond that pertaining to critical infrastructure. ISAOs, including Information Sharing and Analysis Centers (ISACs) have an important role to play in facilitating information sharing going forward and has clarified their functions as defined in the Homeland Security Act.

Section 205. National response framework.

Section 205 amends the Homeland Security Act of 2002 to require the Secretary of the Department of Homeland Security, with proper coordination, to regularly update the Cyber Incident Annex to the National Response Framework of the Department of Homeland Security.

Section 206. Report on reducing cybersecurity risks in DHS data centers.

Section 206 requires the Secretary of the Department of Homeland Security to submit a report to Congress not later than 1 year after the date of the enactment of this Act on the feasibility of using compartmentalization between systems to create conditions conducive to reduced cybersecurity risks in data centers.

Section 207. Assessment.

Section 207 requires the Comptroller General of the United States not later than 2 years after the date of enactment of this Act to submit a report on the implementation of Title II, including increases in the sharing of cyber threat indicators at the National Cybersecurity and Communications Integration Center and throughout the United States.

Section 208. Multiple simultaneous cyber incidents at critical infrastructure.

Section 208 requires the appropriate Department of Homeland Security Under Secretary to draft and submit to Congress not later than 1 year after the date of enactment of this Act a report on the feasibility of producing a risk-informed plan to address the risks of multiple simultaneous cyber incidents affecting critical infrastructure as well as cascade effects.

Section 209. Report on cybersecurity vulnerabilities of United States ports.

Section 209 requires the Secretary of Homeland Security not later than 180 days after the date of enactment of this Act to submit to Congress a report on the vulnerability of United States ports to cybersecurity incidents, as well as potential mitigations.

Section 210. Prohibition on new regulatory authority.

Section 210 clarifies that the Secretary of Homeland Security does not gain any additional regulatory authorities in this subtitle.

Section 211. Termination of reporting requirements.

Section 211 adds a 7-year sunset on the reporting requirements in Title II, Subtitle A.

SUBTITLE B – FEDERAL CYBERSECURITY ENHANCEMENT

Section 221. Short title.

Section 221 establishes that Title II, Subtitle B may be cited as the "Federal Cybersecurity Enhancement Act of 2015".

Section 222. Definitions.

Section 222 defines for purposes of Title II, Subtitle B, the terms "agency," "agency information system," "appropriate congressional committees," "cybersecurity risk," "information system," "Director," "intelligence community," "national security system," and "Secretary."

Section 223. Improved Federal network security.

Section 223 amends the Homeland Security Act of 2002 by amending Section 228, as redesignated, to require an intrusion assessment plan for Federal agencies and adding a Section 230 to authorize a federal intrusion detection and prevention capabilities" for Federal agencies.

Section 230 of the Homeland Security Act of 2002, as added by Section 223(a) of the bill, authorizes the Secretary of Homeland Security to employ the Department's intrusion detection and intrusion prevention capabilities, operationally implemented under the "EINSTEIN" programs, to scan agencies' network traffic for malicious activity and block it. The Secretary and agencies with sensitive data are expected to confer regarding the sensitivity of, and statutory protections otherwise applicable to, information on agency information systems. The Secretary is expected to ensure that the policies and procedures developed under section 230 appropriately restrict and limit Department access, use, retention, and handling of such information to protect the privacy and confidentiality of such information, including ensuring that the Department protects such sensitive data from disclosure, and trains appropriate staff accordingly.

Section 223(b) mandates that agencies deploy and adopt those capabilities within one year for all network traffic traveling to or from each information system owned or operated by the agency, or two months after the capabilities are first made available to the agency, whichever is later. The subsection also requires that agencies adopt improvements added to the intrusion detection and prevention capabilities six months after they are made available. Improvements is intended to be read broadly to describe expansion of the capabilities, new systems, and added technologies, for example: non-signature based detection systems such as heuristic- and behavior-based detection, new countermeasures to block malicious traffic beyond e-mail filtering and Domain Name System (DNS)-sinkholing[1], and scanning techniques that allow scanning of encrypted traffic.

Section 224. Advanced internal defenses.

Section 224 directs the Secretary of Homeland Security to add advanced network security tools to the Continuous Diagnostics and Mitigation program; develop and implement a plan to ensure agency use of advanced network security tools; and, with the Director of the Office of Management and Budget, prioritize advanced security tools and update metrics used to measure security under the Federal Information Security Management Act of 2002.

Section 225. Federal cybersecurity requirements.

Section 225 adds a statutory requirement for the head of each agency not later than 1 year after the date of the enactment of this Act to implement several standards on their networks to include identification of sensitive and mission critical data, use of encryption, and multi-factor authentication.

[1] Use of a DNS server configured to direct attackers away from network infrastructure.

Section 226. Assessment; reports.

Section 226 includes a requirement for a Government Accountability Office study to be conducted on the effectiveness of this approach and strategy. It also requires reports from the Department of Homeland Security, Federal Chief Information Officer, and the Office of Management and Budget. Required reporting includes an annual report from the Department of Homeland Security on the effectiveness and privacy controls of the intrusion detection and prevention capabilities; information on adoption of the intrusion detection and capabilities at agencies in the Office of Management and Budget's annual Federal Information Security Management Act report; an assessment by the Federal Chief Information Officer within two years of enactment as to continued value of the intrusion detection and prevention capabilities; and a Government Accountability report in three years on the effectiveness of Federal agencies' approach to securing agency information systems.

Section 227. Termination.

Section 227 creates a 7-year sunset for the authorization of the intrusion detection and prevention capabilities in Section 230 of the Homeland Security Act of 2002, as added by Section 223(a).

Section 228. Identification of information systems relating to national security.

Section 228 requires the Director of National Intelligence and the Director of the Office of Management, in coordination with other agencies, not later than 180 days after the date of enactment of this Act to identify unclassified information systems that could reveal classified information, and submit a report assessing the risks associated with a breach of such systems and the costs and impact to designate such systems as national security systems.

Section 229. Direction to agencies.

Section 229 authorizes the Secretary of Homeland Security to issue an emergency directive to the head of an agency to take any lawful action with respect to the operation of an information system for the purpose of protecting such system from an information security threat. In situations in which the Secretary has determined there is an imminent threat to an agency, the Secretary may authorize the use of intrusion detection and prevention capabilities in accordance with established procedures, including notice to the affected agency.

TITLE III–FEDERAL CYBERSECURITY WORKFORCE ASSESSMENT

Section 301. Short title.

Section 301 establishes Title III may be cited as the "Federal Cybersecurity Workforce Assessment Act of 2015".

Section 302. Definitions.

Section 302 defines for purposes of Title III the terms "appropriate congressional committees," "Director," "National Initiative for Cybersecurity Education," and "work roles."

Section 303. National cybersecurity workforce measurement initiative.

Section 303 requires the head of each Federal agency to identify all positions within the agency that require the performance of cybersecurity or other cyber-related functions, and report the percentage of personnel in such positions holding the appropriate certifications, the level of preparedness of personnel without certifications to take certification exams, and a strategy for mitigating any identified certification and training gaps.

Section 304. Identification of cyber-related work roles of critical need.

Section 304 requires the head of each Federal agency to identify information technology, cybersecurity, or other cyber-related roles of critical need in the agency's workforce, and substantiate as such in a report to the Director of the Office of Personnel Management. Section 304 also requires the Director of the Office of Personnel Management to submit a subsequent report not later than 2 years after the date of the enactment of this Act, on critical needs for information technology, cybersecurity, or other cyber-related workforce across all Federal agencies, and the implementation of this section.

Section 305. Government Accountability Office status reports.

Section 305 requires the Comptroller General of the United States to analyze and monitor the implementation of sections 303 and 304 and not later than 3 years after the date of the enactment of this Act submit a report on the status of such implementation.

TITLE IV–OTHER CYBER MATTERS

Section 401. Study on mobile device security.

Section 401 requires the Secretary of Homeland Security not later than 1 year after the date of the enactment of this Act to conduct a study on threats relating to the security of the mobile devices used by the Federal Government, and submit a report detailing the findings and recommendations arising from such study.

Section 402. Department of State international cyberspace policy strategy.

Section 402 requires the Secretary of State not later than 90 days after the date of the enactment of this Act to produce a comprehensive strategy relating to United States international policy with regard to cyberspace, to include a review of actions taken by the Secretary of State in support of the President's International Strategy for Cyberspace and a description of threats to United States national security in cyberspace.

Section 403. Apprehension and prosecution of international cyber criminals.

Section 403 requires the Secretary of State, or a designee, to consult with countries in which international cyber criminals are physically present and extradition to the United States is unlikely, to determine what efforts the foreign country has taken to apprehend, prosecute, or otherwise prevent the carrying out of cybercrimes against United States persons or interests. Section 403 further requires an annual report that includes statistics and extradition status about such international cyber criminals.

Section 404. Enhancement of emergency services.

Section 404 requires the Secretary of Homeland Security not later than 90 days after the date of the enactment of this Act to establish a process by which a Statewide Interoperability Coordinator may report data on any cybersecurity risk or incident involving any information system or network used by emergency response providers within the state. Reported data will be analyzed and used in developing information and recommendations on security and resilience on measures for information systems and networks used by state emergency response providers.

Section 405. Improving cybersecurity in the health care industry.

Section 405 requires the Secretary of Health and Human Services to establish a task force and not later than 1 year after the date of enactment of the task force to submit a report on the Department of Health and Human Services and the health care industry's preparedness to respond to cybersecurity threats. In support of the report, the Secretary of Health and Human Services will convene health care industry stakeholders, cybersecurity experts, and other appropriate entities, to establish a task force for analyzing and disseminating information on industry-specific cybersecurity challenges and solutions.

Consistent with subsection (e), it is Congress's intention to allow Health and Human Services the flexibility to leverage and incorporate ongoing activities as of the day before the date of enactment of this act to accomplish the goals set forth for this task force.

Section 406. Federal computer security.

Section 406 requires the Inspector General of any agency operating a national security system, or a Federal computer system that provides access to personally identifiable information, not later than 240 days after the date of enactment of this Act to submit a report regarding the federal computer systems of such agency, to include information on the standards and processes for granting or denying specific requests to obtain and use information and related information processing services, and a description of the data security management practices used by the agency.

Section 407. Stopping the fraudulent sale of financial information of people of the United States.

Section 407 amends 18 U.S. Code § 1029 by enabling the Federal Government to prosecute overseas criminals who profit from financial information that has been stolen from Americans.