Legislative Language

SECTION 1. DEPARTMENT OF HOMELAND SECURITY CYBERSECURITY AUTHORITY.—

Title II of the Homeland Security Act of 2002 (section 121 et seq. of title 6, United States Code) is amended—

(a) in section 201(c) by striking "or the Assistant Secretary for Infrastructure Protection, as appropriate," and inserting "and the Under Secretary responsible for overseeing critical infrastructure protection, cybersecurity, and other related programs of the Department, as appropriate."; and

(b) by adding at the end the following:

‘‘**Subtitle E – Cybersecurity Programs**

‘‘**SEC. 241. SHORT TITLE.**

‘‘**SEC. 242. DEFINITIONS.**

‘‘In this subtitle:

‘‘ (1) The terms "electronic communication," "electronic communication service," and "wire communication" have the meanings set forth for such terms in section 2510 of title 18, United States Code.

‘‘ (2) AGENCY. —The term "agency" has the meaning given that term in section 3552 of title 44, United States Code, as amended.

‘‘(3) COMMUNICATION.—The term "communication" means any electronic communication or wire communication transiting to or from or stored on a federal system or critical information infrastructure.

‘‘(4) COUNTERMEASURE.—The term "countermeasure" means automated actions with defensive intent to modify or block data packets associated with electronic or wire communications, Internet traffic, program code, or other system traffic transiting to or from or stored on an information system for the purpose of protecting the information system from cybersecurity threats when conducted on an information system or information systems owned or operated by or on behalf of the party to be protected or operated by a private entity acting as a provider of electronic communication services, remote computing services, or cybersecurity services to the party to be protected.

‘‘(5) CRITICAL INFRASTRUCTURE.—The term "critical infrastructure" has the meaning given that term in section 5195c(e) of title 42, United States Code.

‘‘ (6) CRITICAL INFORMATION INFRASTRUCTURE.—The term "critical information infrastructure" means any physical or virtual information system that

controls, processes, transmits, receives or stores electronic information in any form including data, voice or video that is—

‘‘ (A) vital to the functioning of critical infrastructure;

‘‘ (B) so vital to the United States that the incapacity or destruction of such systems would have a debilitating impact on national security, national economic security, or national public health or safety; or

‘‘ (C) owned or operated by or on behalf of a state, local, tribal, or territorial government entity.

“ Except that the term “critical information infrastructure” shall not include agency information systems, including federal systems, national security systems, or information systems under the control of the Department of Defense.

‘‘(7) CYBERSECURITY SERVICES.—The term “cybersecurity services” means products, goods, or services used to detect or prevent activity intended to result in unauthorized access to, manipulation of, or impairment to the integrity, confidentiality, or availability of an information system or information stored on or transiting an information system, or unauthorized exfiltration of information stored on or transiting an information system.

‘‘(8) CYBERSECURITY THREAT.— The term “cybersecurity threat” means any action that may result in unauthorized access to, manipulation of, or impairment to the integrity, confidentiality, or availability of an information system or information stored on or transiting an information system, or unauthorized exfiltration of information stored on or transiting an information system.

‘‘(9) FEDERAL SYSTEMS.—The term “federal systems” means all information systems owned, operated, leased, or otherwise controlled by an agency, except for national security systems or those information systems under the control of the Department of Defense.

‘‘(10) INCIDENT.—The term “incident” has the meaning given that term in section 3552 of title 44, United States Code, as amended.

‘‘(11) INFORMATION SECURITY.—The term “information security” has the meaning given that term in section 3552 of title 44, United States Code, as amended.

‘‘(12) INFORMATION SYSTEM.—The term “information system” has the meaning given that term in section 3552 of title 44, United States Code, as amended.

‘‘(13) GOVERNMENTAL ENTITY.—The term “governmental entity” has the meaning given that term in section 2711 of title 18, United States Code.

‘‘(14) NATIONAL SECURITY SYSTEM.—The term “national security system” has the meaning given that term in section 3552 of title 44, United States Code.

‘‘(15) PRIVATE ENTITY.—The term “private entity” means any entity other than a governmental entity as defined in section 2711(4) of title 18, United States Code.

‘‘(16) PROTECT.—The term “protect” means those actions undertaken to secure, defend, or reduce the vulnerabilities of an information system, mitigate cybersecurity threats, or otherwise enhance information security or the resiliency of information systems or assets.

‘‘SEC. 243. ENHANCEMENT OF NATIONAL CYBERSECURITY AND CYBER INCIDENT RESPONSE.

‘‘ (a) IN GENERAL.—The Secretary shall engage in cybersecurity, and other infrastructure protection activities under this title, to support the functioning of federal systems and critical information infrastructure in the interests of national security, national economic security, and national public health and safety.

‘‘ (b) APPROACH.—In carrying out the responsibilities under this subtitle and section 201 of this Act, the Secretary, as appropriate, shall develop and maintain risk-informed approaches that—

‘‘ (1) improve, on an ongoing basis, the information security of federal systems and critical information infrastructure, with particular attention to addressing high consequence risks to national interests;

‘‘ (2) consider the economic competitiveness of United States industry, including the information and communications industries;

‘‘ (3) promote the development and implementation of technical capabilities in support of national cybersecurity goals;

‘‘ (4) minimize the impact of the activities carried out under this subtitle on privacy and civil liberties consistent with section 248(a);

‘‘ (5) promote greater research, innovation, training, education, outreach, public awareness, and investment in cybersecurity; and

‘‘ (6) foster the development of secondary markets and widespread adoption of cybersecurity technology by critical information infrastructure.

‘‘ (c) AUTHORITY AND RESPONSIBILITY TO CONDUCT CYBERSECURITY ACTIVITIES.—To protect federal systems and critical information infrastructure and prepare the nation to respond to, recover from, and mitigate against incidents involving such systems and infrastructure, the Secretary shall, in accordance with this subtitle—

‘‘ (1) create appropriate programs to carry out the purpose and responsibilities under this subtitle;

‘‘ (2) develop and conduct risk assessments that may include threat, vulnerability, and impact assessments, and penetration testing for federal systems and, upon request, critical information infrastructure in consultation with the heads of other

agencies or governmental and private entities that own and operate such systems and infrastructure;

‘‘ (3) foster the development, in conjunction with other governmental entities and the private sector, of essential information security technologies and capabilities for protecting federal systems and critical information infrastructure, including comprehensive protective capabilities and other technological solutions;

‘‘ (4) acquire, integrate, and facilitate the adoption of new cybersecurity technologies and practices to keep pace with emerging cybersecurity threats and developments, including through research and development, technology leasing arrangements, technical service agreements, and making such technologies available to governmental and private entities that own or operate critical information infrastructure, with or without reimbursement, as necessary to accomplish the purpose of this section;

‘‘ (5) designate and maintain a center to serve as a focal point within the federal government for cybersecurity, having responsibilities that include the protection of federal systems and critical information infrastructure and the coordination of cyber incident response, that will—

> ‘‘ (A) facilitate information sharing, interaction and collaboration among and between agencies; State, local, tribal and territorial governments; the private sector; academia and international partners;
>
> ‘‘ (B) work with appropriate agencies; State, local, tribal and territorial governments; the private sector; academia; and international partners to prevent and respond to cybersecurity threats and incidents involving federal systems and critical information infrastructure pursuant to the national cyber incident response plan and supporting plans developed in accordance with paragraph (9);
>
> ‘‘ (C) disseminate timely and actionable cybersecurity threat, vulnerability, mitigation and warning information, including alerts, advisories, indicators, signatures, and mitigation and response measures, to improve the security and protection of federal systems and critical information infrastructure;
>
> ‘‘ (D) integrate information from Federal Government and nonfederal network operation centers and security operations centers to provide situational awareness of the Nation’s information security posture and foster information security collaboration among information system owners and operators;
>
> ‘‘ (E) compile and analyze information about risks and incidents that threaten federal systems and critical information infrastructure, including information voluntarily submitted in accordance with section 245 or otherwise in accordance with applicable laws; and
>
> ‘‘ (F) provide incident detection, analysis, mitigation, and response information and remote or on-site technical assistance to heads of agencies

and, upon request, governmental or private entities that own or operate critical information infrastructure;

‘‘ (6) assist in national efforts to mitigate communications and information technology supply chain vulnerabilities to enhance the security and the resiliency of federal systems and critical information infrastructure;

‘‘ (7) develop and lead a nationwide awareness and outreach effort to educate members of the public about —

‘‘ (A) the importance of cybersecurity;

‘‘ (B) ways to help promote cybersecurity best practices at home and in the workplace;

‘‘ (C) training opportunities to support the development of an effective national cybersecurity workforce; and

“ (D) educational paths to cybersecurity professions;

‘‘ (8) establish in cooperation with the Director of the National Institute of Standards and Technology benchmarks and guidelines for making the critical information infrastructure more secure at a fundamental level, including through automation, interoperability, and privacy-enhancing authentication;

‘‘ (9) develop a national cybersecurity incident response plan and supporting cyber incident response and restoration plans based on applicable law, in collaboration with other relevant agencies; owners and operators of critical information infrastructure; sector coordinating councils; state, local, territorial, and tribal governments; and relevant nongovernmental organizations, that describe the specific roles and responsibilities of governmental and private entities during cyber incidents;

‘‘ (10) develop and conduct exercises, simulations, and other activities designed to support the national response to cybersecurity threats and incidents and evaluate the national cyber incident response plan and supporting plans developed in accordance with paragraph (9); and

‘‘ (11) take such other lawful action as may be necessary and appropriate to accomplish the requirements of this section.

‘‘ (d) COORDINATION AND COOPERATION. —

‘‘ (1) In carrying out the cybersecurity activities under this section, the Secretary shall coordinate, as appropriate, with—

‘‘ (A) the head of any relevant agency or entity;

‘‘ (B) representatives of State, local, tribal, territorial, and foreign governments;

‘‘ (C) the private sector, including owners and operators of critical information infrastructure;

‘‘ (D) academia; and

‘‘ (E) international organizations and foreign partners.

‘‘ (2) The Secretary shall coordinate the activities undertaken by agencies to protect federal systems and critical information infrastructure and prepare the nation to respond to, recover from, and mitigate against risk of incidents involving such systems and infrastructure.

‘‘ (3) The Secretary shall ensure that the Department’s cybersecurity activities under this subtitle are coordinated with all other infrastructure protection and cyber-related programs and activities of the Department, including those of any intelligence or law enforcement components or entities within the Department.

“(e) NO RIGHT OR BENEFIT. –- The provision of assistance or information to governmental or private entities under this section that own or operate critical information infrastructure shall be at the discretion of the Secretary. The provision of certain assistance or information to one governmental or private entity pursuant to this section shall not create a right or benefit, substantive or procedural, to similar assistance or information for any other governmental or private entity.

“(f) SAVINGS CLAUSE. —Nothing in this subtitle shall be interpreted to alter or amend the law enforcement or intelligence authorities of any agency.

‘‘**SEC. 244. NATIONAL CYBERSECURITY PROTECTION PROGRAM.—**

‘‘ (a) In furtherance of the responsibilities assigned under section 243, the Secretary shall protect federal systems from cybersecurity threats by carrying out a cybersecurity program that may include—

‘‘ (1) operating consolidated intrusion detection, prevention, or other protective capabilities and using associated countermeasures for the purpose of protecting federal systems from cybersecurity threats;

‘‘ (2) conducting the risk assessments, including threat, vulnerability, and impact assessments, and penetration testing, on federal systems consistent with section 243(c)(2);

“ (3) providing incident detection, analysis, mitigation, and response information and remote or on-site technical assistance to federal system owners and operators consistent with section 243(c)(5)(F);

‘‘ (4) ensuring common situational awareness of cybersecurity threats and incidents across federal systems to support the protection of federal systems and the operation and defense of external access points across all federal systems;

‘‘ (5) directing, pursuant to section 249, that agencies that own or operate a federal system take action with respect to the operation of such system for the purpose of protecting that system or mitigating a cybersecurity threat;

‘‘ (6) discharging the responsibilities for federal information security set forth in chapter 35 of title 44, United States Code, including the establishment of reporting requirements regarding incidents that impair the adequate security of agency information systems and designation of an entity to receive reports and

information about agency information security incidents, threats, and vulnerabilities affecting agency information systems; and

‘‘ (7) testing and evaluating, consistent with applicable law, information security improvements within the Department.

‘‘ (b) While carrying out the program authorized in subsection (a), the Secretary is authorized, notwithstanding any other provision of law and consistent with section 248(a), to acquire, intercept, retain, use, and disclose communications and other system traffic that are transiting to or from or stored on federal systems and to deploy countermeasures with regard to such communications and system traffic provided that the Secretary certifies that—

‘‘ (1) such acquisitions, interceptions, and countermeasures are reasonably necessary for the purpose of protecting federal systems from cybersecurity threats;

‘‘ (2) the content of communications will be collected and retained only when the communication is associated with a known or reasonably suspected cybersecurity threat, and communications and system traffic will not be subject to the operation of a countermeasure unless associated with such threats;

‘‘ (3) information obtained pursuant to activities authorized under this subsection will only be retained, used or disclosed to protect federal systems from cybersecurity threats, mitigate against such threats, or, with the approval of the Attorney General, for law enforcement purposes when the information is evidence of a crime that has been, is being, or is about to be committed;

‘‘ (4) the communications and system traffic to be acquired, intercepted, retained, used or disclosed are transiting to or from or stored on a federal system;

‘‘ (5) notice has been provided to users of federal systems concerning the potential for acquisition, interception, retention, use, and disclosure of communications and other system traffic; and

‘‘ (6) the cybersecurity program, including the acquisition, interception, retention, use, and disclosure of communications and other system traffic, is implemented consistent with section 248(a).

‘‘ (c) Agencies are authorized to permit the Secretary to acquire, intercept, retain, use, and disclose communications, system traffic, records, or other information transiting to or from or stored on a federal system, notwithstanding any other provision of law, for the purpose of protecting federal systems from cybersecurity threats or mitigating such threats in connection with the implementation of the cybersecurity program authorized by this section.

‘‘ (d) Any certification issued under subsection (b) is valid for up to one year. The Secretary may extend any such authorization for additional periods of up to one year in the same manner required for the original certification.

‘‘ (e) The Secretary may request and obtain the assistance of private entities that provide electronic communications or cybersecurity services to implement this program. The

Secretary shall ensure, by written agreement, that such assistance is conducted consistent with section 248(a).

‘‘ (f) Agencies shall implement this program in accordance with the Secretary’s certification and the requirements of this subtitle. The acquisition, interception, retention, use, or disclosure of communications, record, system traffic and other information by officers, employees, or agents of any agency under this section in a manner not authorized by this section or in accordance with the Secretary’s certification shall be a violation of this subtitle.

‘‘ (g) In implementing the cybersecurity program authorized in subsection (a) and activities authorized in subsection (b), the Secretary shall coordinate with heads of appropriate agencies, including those responsible for federal systems, to accomplish the purposes of this section consistent with agency mission requirements.

‘‘ SEC. 245. VOLUNTARY DISCLOSURE OF CYBERSECURITY INFORMATION.—

‘‘ (a)(1) A nonfederal governmental or private entity, or any officer, employee, or agent thereof, that lawfully intercepts, acquires, or otherwise obtains or possesses any communication, record, or other information, notwithstanding any other provision of law and consistent with section 248(a), may disclose that communication, record, or other information to the cybersecurity center designated by the Secretary under section 243(c)(5) for the purpose of protecting an information system from cybersecurity threats or mitigating such threats, provided that reasonable efforts are undertaken to remove information that can be used to identify specific persons unrelated to the cybersecurity threat before any disclosure.

> ‘‘ (2) An agency, or any officer, employee, or agent thereof, that lawfully intercepts, acquires, or otherwise obtains or possesses any communication, record, or other information from its electronic communications system, notwithstanding any other provision of law and consistent with section 248(b), may disclose that communication, record, or other information to—
>
> > ‘‘ (A) another component, officer, employee, or agent of that agency with cybersecurity responsibilities;
> >
> > ‘‘ (B) the cybersecurity center designated by the Secretary under section 243(c)(5); or
> >
> > ‘‘ (C) a private entity that is acting as a provider of electronic communication services, remote computing service, or cybersecurity services to the agency
>
> for the purpose of protecting an agency information system from cybersecurity threats or mitigating cybersecurity threats.

‘‘ (b)(1) The Department may only use, retain or further disclose information to appropriate governmental and private entities obtained pursuant to this section, consistent with section 248(a), in order to protect information systems from cybersecurity threats, mitigate cybersecurity threats, or, with the approval of the Attorney General, to law

enforcement entities when the information is evidence of a crime that has been, is being, or is about to be committed.

‘‘ (2) Agencies receiving communications, records or other information from the Department pursuant to paragraph (1) shall only use or retain such communications, records or other information consistent with section 248(b) protect agency information systems from cybersecurity threats, mitigate cybersecurity threats, or, with the approval of the Attorney General, for law enforcement purposes when the information is evidence of a crime which has been, is being, or is about to be committed.

‘‘ (c) Agencies shall ensure, by written agreement, that when disclosing communications, records, or other information to nonfederal governmental or private entities under this section, such nonfederal governmental or private entities use or retain such communications, records, or other information consistent with section 248(a) and for the purpose of protecting information systems from cybersecurity threats, mitigating cybersecurity threats, or for law enforcement purposes when the information is evidence of a crime which has been, is being, or is about to be committed. The Attorney General shall approve any disclosures for law enforcement purposes prior to disclosure.

‘‘ (d) Nothing in this section shall limit or prohibit otherwise lawful disclosures of communications, records, or information by a private entity to the Department or any other governmental or private entity not conducted under this section.

“ (e) Nothing in this section permits the unauthorized disclosure of information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations; any restricted data, as defined in paragraph y. of section 11 of the Atomic Energy Act of 1954; information related to intelligence sources and methods; or information that is specifically subject to a court order or a certification, directive, or other authorization by the Attorney General precluding such disclosure.

‘‘ (f) Any communication, record, or other information disclosed by a State or local government entity or a private entity to the Department pursuant to subsection (a) shall be exempt from disclosure under section 552(b)(3) of title 5, United States Code, or any comparable state law. Such communications, records, and other information shall be treated as voluntarily shared information under section 552 of title 5, United States Code, and any comparable state law.

‘‘ (g) The disclosure or use of communications under this section in a manner not authorized by this section shall be a violation of this subtitle.

SEC. 246. LIMITATION ON LIABILITY AND GOOD FAITH DEFENSE FOR CYBERSECURITY ACTIVITIES.—

‘‘ (a) No civil or criminal cause of action shall lie or be maintained in any Federal or State court against any nonfederal governmental or private entity, or any officer, employee, or agent thereof, for—

‘‘ (1) the disclosure of any communication, record, or other information authorized by this subtitle; or

‘‘ (2) any assistance provided to the Department pursuant to section 244(e),

and any such action shall be dismissed promptly.

‘‘ (b) Where a civil or criminal cause of action is not barred under subsection (a), a good faith reliance by any person on a legislative authorization, a statutory authorization, or a good faith determination that this subtitle permitted the conduct complained of, is a complete defense against any civil or criminal action brought under this subtitle or any other law.

SEC. 247. FEDERAL PREEMPTION, EXCLUSIVITY, AND LAW ENFORCEMENT ACTIVITIES.—

‘‘ (a) This subtitle supersedes any statute of a State or political subdivision of a State that restricts or otherwise expressly regulates the acquisition, interception, retention, use or disclosure of communications, records, or other information by private entities or governmental entities to the extent such statute is inconsistent with this subtitle.

‘‘ (b) Section 244(b) shall constitute an additional exclusive means for the domestic interception of wire or electronic communications, in accordance with section 1812(b) of title 50, United States Code.

“ (c) This subtitle does not authorize the Secretary to engage in law enforcement or intelligence activities that the Department is not otherwise authorized to conduct under existing law.

SEC. 248. PRIVACY AND CIVIL LIBERTIES; OVERSIGHT; PENALTIES FOR MISUSE.—

‘‘ (a) In consultation with privacy and civil liberties experts, the Secretary shall develop and periodically review policies and procedures governing the acquisition, interception, retention, use, and disclosure of communications, records, system traffic, or other information associated with specific persons by officers, employees, and agents of the Department obtained in connection with activities authorized in this subtitle. The policies and procedures developed under this subsection shall be reviewed and approved by the Attorney General. Such policies and procedures shall—

‘‘ (1) minimize the impact on privacy and civil liberties, consistent with the need to protect federal systems and critical information infrastructure from cybersecurity threats and mitigate cybersecurity threats;

‘‘ (2) reasonably limit the acquisition, interception, retention, use and disclosure of communications, records, system traffic, or other information associated with specific persons consistent with the need to carry out the responsibilities of this subtitle, including establishing a process for the timely destruction on recognition of communications, records, system traffic or other information that is acquired or intercepted pursuant to this section that does not reasonably appear to be related

to protecting federal systems and critical information infrastructure from cybersecurity threats and mitigating cybersecurity threats;

‘‘ (3) include requirements to safeguard communications, records, system traffic or other information that can be used to identify specific persons from unauthorized access or acquisition; and

“(4) protect the confidentiality of disclosed communications, records, system traffic, or other information associated with specific persons to the greatest extent practicable and require recipients of such information to be informed that the communications, records, system traffic or other information disclosed may only be used for protecting information systems against cybersecurity threats, mitigating against cybersecurity threats, or law enforcement purposes when the information is evidence of a crime that has been, is being, or is about to be committed, as specified by the Secretary.

‘‘ (b) In consultation with privacy and civil liberties experts, and consistent with the requirements of subsection (a), the head of each agency shall develop and periodically review policies and procedures governing the acquisition, retention, use, and disclosure of communications, records, system traffic or other information associated with specific persons by officers, employees, and agents of the agency obtained or disclosed in connection with activities authorized in this subtitle. The policies and procedures developed under this subsection shall be reviewed and approved by the Attorney General within one year of the effective date of this Act.

‘‘ (c) The head of each agency shall establish a program to monitor and oversee compliance with the policies and procedures issued under subsection (a) or (b), respectively. The head of the agency shall promptly notify the Attorney General of significant violations of such policies and procedures, and shall provide the Attorney General with any information relevant to the violation that the Attorney General requires.

‘‘ (d) The policies and procedures under subsection (a) or (b) and any amendments thereto shall be provided to the Congress.

‘‘ (e) On an annual basis, the Chief Privacy and Civil Liberties Officer of the Department of Justice and the Department, in consultation with the most senior privacy and civil liberties officer or officers of appropriate agencies, shall submit a joint report to the Congress assessing the privacy and civil liberties impact of the governmental activities conducted pursuant to this subtitle.

‘‘ (f) Two years after enactment of this provision, the Privacy and Civil Liberties Oversight Board shall submit a report to the Congress and the President providing its assessment of the privacy and civil liberties impact of the government’s activities under this subtitle and recommending improvements to or modifications of the law to address privacy and civil liberties concerns.

‘‘ (g) No communications, records, system traffic or other information acquired or collected pursuant to this subtitle may be used, retained, or disclosed by governmental or private entities except as authorized under this subtitle.

“ (h) No otherwise privileged communication obtained in accordance with, or in violation of, the provisions of this subtitle shall lose its privileged character.

“ (i) The heads of agencies shall develop and enforce appropriate sanctions for officers, employees, or agents of the agency who conduct activities under this subtitle—

‘‘ (1) outside the normal course of their specified duties;

‘‘ (2) in a manner inconsistent with the discharge of the agency’s responsibilities; or

‘‘ (3) in contravention of policies and procedures under subsection (a) or (b), respectively.

“ (j) Any person who knowingly and willfully violates restrictions under this subtitle with respect to acquisition, interception, use, retention, or disclosure of communications, records, system traffic or other information, or the related procedures established pursuant to subsection (a) or (b), shall be guilty of a misdemeanor and fined not more than $5,000 per incident.

“SEC. 249. REQUIRED SECURITY ACTION.—

“ (a) In response to a known or reasonably suspected cybersecurity threat or incident, the Secretary may direct officials of agencies that own or operate a federal system to take any lawful action with respect to the operation of such system for the purpose of protecting that system from or mitigating a cybersecurity threat. The Secretary shall—

“ (1) establish, in coordination with the Director of the Office of Management and Budget, procedures governing the circumstances under which such directive may be issued under this section, including—

“ (A) thresholds and other criteria;

“ (B) privacy and civil liberties protections consistent with section 248(a); and

“ (C) notice to potentially affected third parties as may be applicable;

“ (2) specify the reasons for the required action and the duration of such directive;

“ (3) minimize the impact of directives under this section by adopting the least intrusive means possible to secure the federal system or systems under the particular circumstances for the shortest time practicable; and

“ (4) notify the Director of the Office of Management and Budget and head of any affected agency immediately upon the issuance of directives under this section.

“ (b) When the Secretary determines that there is an imminent threat to federal systems and a directive under subsection (a) is not reasonably likely to result in a timely response to the threat, the Secretary may, without prior consultation with the affected agency, authorize use of protective capabilities under the Secretary’s control on communications or other system traffic transiting to or from or stored on a federal system for the purpose of ensuring the security of that system or other federal systems, provided that—

“ (1) the authorities under this subsection are not delegated below the level of Assistant Secretary;

“ (2) the Secretary or the Secretary’s designee immediately notifies the Director of the Office of Management and Budget, head of the affected agencies, and associated Chief Information Officers of any action taken under this subsection as to the reasons, duration, and nature of the action; and

“ (3) the Secretary’s actions are otherwise consistent with applicable law.