SECTION-BY-SECTION

Section 1. Short Title. The short title of the bill is the "Cybersecurity Act of 2012".

Section 2. Definitions. Section 2 defines terms including "commercial information technology product", "commercial item", "covered critical infrastructure", "covered system or asset", "critical infrastructure", "Federal information infrastructure", "incident", "information infrastructure", "information sharing and analysis organization", "information system", "institution of higher education", "intelligence community", "national information infrastructure", "national security system", "owner", and "operator."

TITLE I. PROTECTING CRITICAL INFRASTRUCTURE

Section 101. Definitions and Responsibilities. Section 101 defines terms including "cyber risk" and "sector-specific agency" and specifies that it is the responsibility of the owner of critical infrastructure covered under this bill to comply with the Act's requirements.

Section 102. Sector-by-Sector Cyber Risk Assessments. Section 102 requires the Secretary of Homeland Security, in consultation with owners and operators of critical infrastructure, the Critical Infrastructure Partnership Advisory Council, sector-specific agencies, and others, to conduct a top level assessment of cybersecurity risks to determine which sectors face the greatest immediate risk, and beginning with the sectors identified as the highest priority, conduct, on a sector-by-sector basis, cyber risk assessments of critical infrastructure.

Section 103. Procedure for Designation of Covered Critical Infrastructure. Section 103 requires the Secretary of Homeland Security, in consultation with owners and operators of critical infrastructure, the Critical Infrastructure Partnership Advisory Council, sector-specific agencies, and others, to establish a procedure for the designation of covered critical infrastructure on a system or asset level. The section directs the Secretary to designate covered critical infrastructure on the system or asset level and to designate a system or asset as covered critical infrastructure only if a cyber attack to that system or asset could reasonably result in: (1) interruption of life-sustaining services sufficient to cause a mass casualty event or mass evacuations; (2) catastrophic economic damage to the United States; or (3) severe degradation of national security. The section prohibits the Secretary of Homeland Security from designating a commercial information technology product itself, including hardware and software, as covered critical infrastructure while recognizing that such products could be components of a covered system. The section also requires the Secretary to develop a mechanism for redress of the designation of a system or asset as covered critical infrastructure.

Section 104. Sector-by-Sector Risk-Based Cybersecurity Performance Requirements. Section 104 requires the Secretary of Homeland Security to establish a process to receive proposals on cybersecurity performance requirements from owners and operators of critical infrastructure and others, and to determine if there are any existing regulations that apply to the system or asset. If the Secretary of Homeland Security determines that the proposed performance requirements fail to ensure that owners of covered critical infrastructure will secure a covered system or asset and

there are no existing regulations in place to do so, the Secretary shall, in consultation with owners of critical infrastructure, the Critical Infrastructure Partnership Advisory Council, sector-specific agencies, and others, develop satisfactory performance requirements. The President may exempt covered critical infrastructure from the requirements of this title if he determines that the appropriate sector-specific agency has regulations in place to effectively mitigate the identified cyber risks. The section prohibits regulating the design, development, or manufacture of commercial information technology products.

Section 105. Security of Covered Critical Infrastructure. Section 105 requires measures to ensure the security of covered critical infrastructure, including ensuring that owners of covered critical infrastructure: (1) are regularly informed of cyber risks and threats and appropriate security performance requirements; (2) implement measures the owner determines best satisfy cybersecurity performance requirements and annually self-certify or have a third party assess compliance with the performance requirements; and (3) report significant cyber incidents affecting covered critical infrastructure. The Secretary of Homeland Security may exempt from the performance requirements any system or asset which the owner demonstrates is sufficiently secure from identified cyber risks. An action to enforce the requirements of this section shall be initiated by the Federal agency with responsibilities for regulating the security of covered critical infrastructure, or by the Secretary of Homeland Security if the covered critical infrastructure is not subject to regulation by another agency, or if the head of the Federal agency with responsibility for regulating the security of covered critical infrastructure requests the Secretary of Homeland Security to take such action or fails to take an enforcement action after a request by the Secretary of Homeland Security. The section provides that owners of covered critical infrastructure who are in substantial compliance with cybersecurity performance requirements shall not be liable for any punitive damages arising from an incident related to a cybersecurity risk identified in the assessments under section 102.

Section 106. Sector-Specific Agencies. Section 106 requires the head of each sector-specific agency, the head of any Federal agency with responsibilities for regulating the security of covered critical infrastructure, and the Secretary of Homeland Security to coordinate on activities regarding cybersecurity and avoid duplicative reporting requirements.

Section 107. Protection of Information. Section 107 requires that covered information submitted in accordance with this section be treated as voluntarily shared critical infrastructure information under section 214 of the Homeland Security Act. Covered information in this section includes information that is a trade secret, information submitted in accordance with section 105, and information submitted regarding cyber threats, vulnerabilities, risks and incidents.

Section 108. Voluntary Technical Assistance. Section 108 authorizes the Secretary of Homeland Security to provide voluntary technical assistance at the request of an owner or operator of covered critical infrastructure to assist the owner in meeting the requirements in section 105.

Section 109. Emergency Planning. Section 109 requires the Secretary of Homeland Security, in partnership with owners and operators of covered critical infrastructure and heads of sector-specific agencies, to exercise cyber response and restoration plans.

Section 110. International Cooperation. Section 110 requires the Secretary of Homeland Security, in coordination with the Secretary of State or the head of sector-specific agencies and others, to: (1) inform owners or operators of information infrastructure located outside of the United States, the disruption of which could result in catastrophic damage within the United States, of information related to cyber risks to such information infrastructure; and (2) coordinate with international governments and owners of such information infrastructure regarding mitigation or remediation of cyber risks.

Section 111. Effect on Other Laws. Section 111 provides that this Act shall supersede any statute, provision of a statute, regulation, or rule of a State or political subdivision of a State that expressly requires comparable cybersecurity practices to protect covered critical infrastructure, but preserves all other State laws or requirements.

TITLE II. PROTECTING GOVERNMENT NETWORKS

Section 201. FISMA Reform. Title II amends the Federal Information Security Management Act of 2002 (FISMA) by striking subchapters II and III of chapter 35 of Title 44, United States Code (44 U.S.C. §§ 3541, et seq.), and inserting the following sections. Many of the original FISMA requirements are retained in this language. The section-by-section analysis below refers to the new sections of Title 44, as amended by this bill.

New Section 3551. Purposes. Section 3551 states the purposes of this subchapter are to provide comprehensive policy and oversight framework for federal agencies' information security, while emphasizing the need for continuous monitoring and streamlined reporting.

New Section 3552. Definitions. Section 3552 defines terms, including: "adequate security", "continuous monitoring", "incident", "information security", "information technology", and "national security system".

New Section 3553. Federal Information Security Authority and Coordination. Section 3553 clarifies and builds on DHS's role of overseeing FISMA to increase security and efficiency across the Federal government. It gives DHS statutory authority to match its current responsibilities given by the White House in 2010 to oversee and issue civilian agency information security. It also requires red team exercises and operational testing, gives DHS the ability to streamline agency reporting requirements, and reduces paperwork exercises by moving to continuous monitoring and risk assessment. It gives DHS the authority to issue risk mitigation directives to agencies whose security is lacking. It clarifies the authority and necessary privacy protections for DHS to operate its government-wide intrusion detection and prevention system known as "EINSTEIN," and limits DHS's intrusion prevention role in the case of an imminent threat. Reflecting current law, it would maintain the authority of the Defense Department and Intelligence Community over their own systems, as well as the President's current authorities over national security systems. It requires DHS to coordinate with NIST and the DOD to ensure that its policies are complementary.

New Section 3554. Agency Responsibilities. Section 3554 lays out responsibilities of agency heads to provide adequate security for the information and systems under their control. It requires agency heads to update their information security programs to facilitate a culture of security, rather than a culture of compliance. The programs include continuous monitoring, red team exercises, effective risk management, and information sharing within the Federal space. The section also requires security, privacy, and civil liberties awareness training for agency personnel. Agency heads would report on the effectiveness of their security programs and identify significant deficiencies and processes to remediate those deficiencies.

New Section 3555. Annual Assessments. Section 3555 codifies the annual assessments of agencies' security programs that DHS is currently conducting. These holistic reviews assist agencies in understanding their strengths and weaknesses.

New Section 3556. Independent Evaluations. Section 3556 makes the current inspector general reviews under FISMA more consistent and effective. The guidance developed under this section assists the auditors in focusing on security rather than compliance, resulting in more consistent, risk-based, and cost-effective reviews.

New Section 3557. National Security Systems. Section 3557 maintains the language under current FISMA to ensure that agencies provide security for national security systems.

New Section 3560. Effect on Existing Law. This section clarifies that nothing within the title interferes with other existing laws.

Section 202. Management of Information Technology. Section 202 maintains NIST's current role under FISMA to develop binding information security standards for Federal agencies.

Section 203. Savings Provisions. Section 203 protects the current information security policies of OMB and NIST until they expire or are repealed.

TITLE III. CLARIFYING AND STRENGTHENING EXISTING ROLES AND AUTHORITIES

Section 301. Consolidation of Existing Departmental Cyber Resources and Authorities. Section 301 amends Title II of the Homeland Security Act (HSA) of 2002 to add the sections described below.

New Section 241 of the HSA. Definitions. Section 241 defines terms including "agency information infrastructure", "covered critical infrastructure", "damage", "Federal cybersecurity center", "Federal information infrastructure", "incident", "information security", "information system", "national security and emergency preparedness communications infrastructure", "national information infrastructure", and "national security system".

New Section 242 of the HSA. Consolidation of Existing Resources. Section 242 consolidates several existing functions within DHS—the National Cyber Security Division, the Office of Emergency Communications, and the National Communications Systems—into a newly

established National Center for Cybersecurity and Communications (NCCC or the Center). The Center would be headed by a Director appointed by the President and confirmed by the Senate. The Director would be responsible for managing Federal efforts to secure, protect, and ensure the resiliency of cyber networks in the United States. The Center would have two Deputy Directors, one of whom would be an employee of the Intelligence Community identified by the Director of National Intelligence, in concurrence with the Secretary of Homeland Security. This intelligence-focused deputy would ensure that the knowledge and expertise that resides in the Intelligence Community is integrated into the NCCC from the outset. The Center would also have staff detailed from the Departments of Defense, Justice, and Commerce, as well as the Intelligence Community. To ensure that privacy and civil liberties are taken into account in every aspect of the Center's policy and operations, it would also have a full-time Chief Privacy Officer.

New Section 243 of the HSA. DHS Information Sharing. Section 243 requires the Director of the NCCC, in consultation with the private sector, relevant government agencies, and nongovernmental organizations, to conduct an assessment of existing and proposed information sharing models in order to establish a program to facilitate cybersecurity information sharing. The Director must establish a program for the sharing of both classified and unclassified cybersecurity information with other Federal agencies, the private sector, state and local governments, and international partners. Additionally, the Director of the NCCC, in consultation with the Attorney General, the DNI, and the NCCC's privacy officer must establish and implement guidelines to ensure the protection of privacy and civil liberties.

New Section 244 of the HSA. Access to Information. Section 244 gives the Director of the NCCC access to any information possessed by a Federal agency that is relevant to the security of the Federal information infrastructure. Consistent with applicable law, the Director may also receive such information from State and local governments and private entities.

New Section 245 of the HSA. National Center for Cybersecurity and Communications Acquisition Authorities. New section 245 gives the NCCC the same procurement flexibilities currently available to the Department of Defense, NASA, and the Coast Guard, which allow narrow exceptions to normal competitive procedures for procurements that may be satisfied by a limited number of responsible sources, or for follow-on contracts for the continued provision of highly specialized services. To ensure these exceptions are used only when necessary, this section subjects them to justification and approval procedures, and the authorities would terminate three years after the date of enactment of this Act. The Director must report on a semiannual basis to Congress on the use of the authority granted under this section.

New Section 246 of the HSA. Recruitment and Retention Program for the NCCC. To recruit and retain highly skilled personnel to carry out the mission of the Center, section 246 gives the Secretary of Homeland Security hiring and compensation authorities for cybersecurity employees commensurate with those of the Secretary of Defense under 10 U.S.C. §1601, to establish positions in the excepted service that would permit the Secretary to make direct appointments; 10 U.S.C. §1602, to set rates of basic pay; and 10 U.S.C. §1603, to provide additional compensation, benefits, incentives, and allowances. The section also authorizes the Secretary to exercise, with respect to cybersecurity employees, the same authorities as the

Secretary of Defense to establish a scholarship program to enable employees to pursue an associate, baccalaureate, or advanced degree, or a certification in an information assurance discipline. The section requires the Secretary to report to Congress annually on the process used to hire individuals for cybersecurity positions and how the Secretary plans to fill the critical need of DHS to recruit and retain skilled cybersecurity employees.

New Section 247 of the HSA. Prohibited Conduct. This section prohibits the Federal government from compelling the disclosure of information from a private entity relating to an incident unless otherwise authorized by law and from intercepting a wire, oral, or electronic communication relating to an incident unless otherwise authorized by law.

TITLE IV. EDUCATION, RECRUITMENT, AND WORKFORCE DEVELOPMENT

Section 401. Definitions. Section 401 defines the terms "cybersecurity mission" and "cybersecurity mission of a Federal agency."

Section 402. National Education and Awareness Campaign. Section 402 requires the Secretary of Homeland Security and the Director of the National Institute of Standards and Technology to develop and implement an outreach and awareness program on cybersecurity to increase understanding of the benefits of cybersecurity measures.

Section 403. National Cybersecurity Competition and Challenge. Section 403 requires the Secretary of Homeland Security and the Secretary of Commerce to establish a program to advance national and statewide competitions and challenges that seek to identify, develop, and recruit talented individuals to work in federal, state, and local governments, and the private sector on cybersecurity.

Section 404. Federal Cyber Scholarship-for-Service Program. Section 404 directs the Director of the National Science Foundation to establish a Federal Cyber Scholarship-for-Service program to recruit and train cybersecurity professionals to meet the needs of the Federal government's cybersecurity mission.

Section 405. Assessment of Cybersecurity Federal Workforce. Section 405 requires the Director of the Office of Personnel Management (OPM), in coordination with various Federal agencies and others, to assess the readiness and capacity of the Federal workforce to meet the needs of the Federal government's cybersecurity mission.

Section 406. Federal Cybersecurity Occupation Classifications. Section 406 requires the Director of OPM to develop and issue comprehensive occupation classifications for Federal employees engaged in the cybersecurity mission.

Section 407. Training and Education. Section 407 requires the Director of OPM, in coordination with various Federal agencies, to establish a cybersecurity awareness and education curriculum program for all Federal employees and Federal contractors and a program to provide training to improve the technical skills and capabilities of Federal employees engaged in the cybersecurity mission. The section requires the Secretary of Education, working with state and local

governments, to develop model curriculum standards, guidelines, and recommended courses to address cyber safety, cybersecurity, and cyber ethics for students in kindergarten through grade twelve, as well as undergraduate, graduate, vocational, and technical institutions.

Section 408. Cybersecurity Incentives. Section 408 requires each Federal agency to adopt OPM best practices regarding ways to motivate employees to demonstrate leadership in the field of cybersecurity.

TITLE V. RESEARCH AND DEVELOPMENT

Section 501. Federal Cybersecurity Research and Development. Section 501 requires the Director of Science and Technology Policy, in coordination with the Secretary of Homeland Security and the head of any relevant Federal agency, to develop a national cybersecurity research and development plan. The section requires the Director of the Office of Science and Technology Policy to further support research that evaluates secure coding education and improvement programs and new methods of integrating secure coding improvement into the educational core curriculum and to report to Congress on the state of secure coding education in colleges and universities. The section also requires the Director of the Office of Science and Technology Policy to establish a program to provide grants to institutions of higher education to establish cybersecurity test beds capable of realistic modeling of cyber attacks to support development of new cybersecurity defenses. The section also expands the NSF Computer and Network Security Research Grant Areas to improve cybersecurity through secure software engineering. The section reauthorizes the Cybersecurity Faculty Development and Traineeship Program through 2014 and authorizes the development of standards and guidelines for enhanced cybersecurity as part of the Networking and Information Technology Research and Development Program.

Section 502. Homeland Security Cybersecurity Research and Development. Section 502 amends Subtitle D of title II of the Homeland Security Act of 2002 by adding the following section.

New Section 238 of HSA. Cybersecurity Research and Development. Section 238 requires DHS to carry out a research and development program to improve the security of the nation's information infrastructure.

TITLE VI. FEDERAL ACQUISTION RISK MANAGEMENT STRATEGY.

Section 601. Federal Acquisition Risk Management Strategy. Section 601 requires the Secretary of Homeland Security to coordinate with private sector experts, the Secretaries of Defense, Commerce and State, the Director of National Intelligence, and other Federal agencies, to develop an acquisition risk management strategy to ensure the security of Federal networks. The section specifies that this strategy must incorporate all-source intelligence analysis of the integrity of the supply chain for Federal networks, as well as private sector standards, guidelines and best practices.

Section 602. Amendments to Clinger-Cohen Provisions to Enhance Agency Planning for Information Security Needs. Section 602 amends the Clinger-Cohen Act, the Federal law that governs the Federal government's acquisition and management of information technology resources, to enhance agency planning for information security needs. Section 602 is intended to further the practical implementation of the strategy developed in Section 601 and to modernize the law's approach to cybersecurity by ensuring that agencies prioritize security in information technology purchases, keep mandatory security standards up to date, use security best practices, train acquisition officers in information security, root out bureaucratic impediments to purchasing secure technologies, and take new steps to eliminate purchases of counterfeit products.

TITLE VII. INFORMATION SHARING.

Section 701. Affirmative Authority to Monitor and Defend Against Cybersecurity Threats. Section 701 removes legal barriers to sharing information by permitting private entities to monitor and defend their own systems and the systems of a third party, as long as the third party authorizes them to do so, against cybersecurity threats.

Section 702. Voluntary Disclosure of Cybersecurity Threat Indicators among Private Entities. Section 702 permits private entities to disclose or receive lawfully obtained cybersecurity threat information provided they use the information only to protect an information system and make reasonable efforts to safeguard information that can be used to identify specific persons from unauthorized access or acquisition.

Section 703. Cybersecurity Exchanges. Section 703 establishes a process to designate cybersecurity exchanges that will serve as hubs for appropriately distributing, receiving, and exchanging cybersecurity threat information. Specifically, this section requires the Secretary of Homeland Security, in consultation with the Director of National Intelligence, the Attorney General, and the Secretary of Defense, to establish (1) a process for designating appropriate Federal and non-Federal entities as cybersecurity exchanges, (2) procedures to facilitate and encourage the sharing of classified and unclassified cybersecurity threat information, and (3) a process for identifying entities capable of receiving classified cybersecurity threat information. Section 703 also requires the Secretary of Homeland Security, in consultation with the Director of National Intelligence, the Attorney General, and the Secretary of Defense, to designate a lead Federal cybersecurity exchange to serve as the focal point within the Federal Government to facilitate and encourage information sharing with both Federal and non-Federal entities.

Section 704. Voluntary Disclosure of Cybersecurity Threat Indicators to a Cybersecurity Exchange. Section 704 removes legal barriers and permits a non-Federal entity to disclose lawfully obtained cybersecurity threat information to a cybersecurity exchange provided that the information is only used, retained, or disclosed by the cybersecurity exchange to protect an information system from a cyber threat. Additionally, this section prohibits a Federal entity that lawfully intercepts, acquires, or otherwise obtains any information from its electronic communications system from disclosing that information, unless it is made for the specific purpose of protecting a Federal entity's system or a private entity that is providing a cyber service to the Federal Government. Section 704 permits disclosure of cybersecurity threat

information to law enforcement if the information pertains to a crime which has been, is being, or is about to be committed. This section also requires the Secretary of Homeland Security, in consultation with privacy and civil liberties experts, to develop policies governing the receipt, retention, use, and disclosure of cybersecurity threat information by a Federal entity that include procedures to minimize the impact on privacy and civil liberties and safeguard and limit the use of information associated with specific persons. Finally, this section directs the Secretary of Homeland Security and the Attorney General to establish a mandatory program to oversee and monitor compliance with the policies and procedures that protect privacy and civil liberties.

Section 705. Sharing of Classified Cybersecurity Threat Indicators. Section 705 provides that procedures developed to facilitate and encourage information sharing must provide that classified cybersecurity threat information may only be shared with certified entities and appropriately cleared persons in a manner that protects national security. This section directs the Director of National Intelligence to issue guidelines providing that appropriate Federal officials may grant security clearances to certified entities and employees of certified entities.

Section 706. Limitation on Liability and Good Faith Defense for Cybersecurity Activities. Section 706 provides that no cause of action shall lie or be maintained based on the cybersecurity monitoring activities permitted under section 701 or for the voluntary disclosure of lawfully obtained cybersecurity threat information (1) to a cybersecurity exchange, (2) by a provider of cyber services to its customers, (3) to an owner or operator of critical infrastructure, or (4) to a non-Federal entity provided that the information is shared with a cybersecurity exchange within a reasonable time. This section also provides that a good faith reliance that this title permitted the conduct complained of is a complete defense against any cause of action brought. Additionally, section 706 prohibits a cause of action for the reasonable failure to act on information received under the title.

Section 707. Construction; Federal Preemption. Section 707 provides that nothing in the title may be construed to permit price-fixing or market allocation between competitors. Additionally, this section provides that this title preempts any law or requirement of a State or political subdivision of a State that restricts or otherwise expressly regulates the provision of cybersecurity services or the acquisition, interception, retention, use or disclosure of communications, records, or other information by private entities to the extent such law contains requirements inconsistent with this Title, but preserves all other state laws or requirements.

Section 708. Definitions. Section 708 defines terms including, “certified entity”, cybersecurity exchange”, “cybersecurity threat indicator”, “Federal cybersecurity center”, operational control”, “protected entity”, “self-protected entity”, technical control”, and “third party.”

TITLE VIII. PUBLIC AWARENESS REPORTS

Section 801. Findings. Section 801 contains several Congressional findings related to the threat that cyber risks pose to our national security and that the level of public awareness of cybersecurity threats is unacceptably low.

Section 802. Report on Cyber Incidents Against Government Networks. Section 802 requires DHS to report annually to Congress summarizing major cyber incidents against civilian government networks, discussing the risk of cyber sabotage against those networks, and providing aggregate statistics regarding breaches of executive networks. It also requires the Department of Defense to report annually to Congress the same information regarding military networks.

Section 803. Reports on Prosecution for Cybercrimes. Section 803 directs the Attorney General and Director of the FBI to submit an annual report to Congress describing investigations and prosecutions relating to cybercrimes in the preceding year, and discussing any impediments under US or international law to such prosecutions.

Section 804. Research Report Regarding Secure Domain. Section 804 requires the Secretary to contract with the National Research Council, or other federally funded research and development corporation, to submit to Congress annual reports on available constitutionally sound technical options for enhancing the security of information networks of entities that own or manage critical infrastructure.

Section 805. Report on Preparedness of Federal Courts to Promote Cybersecurity. Section 805 requires the Attorney General to submit to Congress a report on whether Federal courts are granting timely relief in matters relating to cybercrime, including recommendations on changes to the Federal Rules of Civil Procedure and Criminal Procedure, training of the Federal judiciary, the specialization of courts, and federal law.

Section 806. Report on Impediments to Public Awareness. Section 806 requires the Secretary to submit an annual report to Congress on the legal or other impediments to public awareness of cybersecurity threats and mitigation methods, a summary of the Secretary's plans to enhance public awareness, and recommendations for congressional action to address these impediments.

Section 807. Report on Protecting the Electrical Grid of the United States. Section 807 requires the Secretary, in consultation with the Secretary of Defense and the Director of National Intelligence, to submit to Congress a report on the threat, implications, options available in the event of, and a plan to prevent disruption of the electric grid of the United States caused by a cyber attack.

TITLE IX – INTERNATIONAL COOPERATION

Section 901. Definitions. Section 901 defines the terms "computer systems," "computer data," "Convention on Cybercrime," "cybercrime," "cyber issues" and "relevant federal agencies."

Section 902. Findings. Section 902 contains several Congressional findings demonstrating the integral role coordinating and collaborating with international partners plays in protecting cyberspace.

Section 903. Sense of Congress. Section 903 expresses the sense of the Congress that international engagement to advance U.S. cyberspace objectives should be an integral part of U.S. foreign relations and diplomacy and that the Secretary of State should lead this U.S. effort.

Section 904. Coordination of International Cyber Issues Within the United States Government. Section 904 authorizes the Secretary of State to designate a senior level State Department official to coordinate U.S. diplomatic engagement on international cyber issues, provide strategic direction and coordination for U.S. policy on international cyber issues, and coordinate with relevant Federal agencies to develop interagency plans regarding international cybersecurity.

Sec. 905. Consideration of Cybercrime in Foreign Policy and Foreign Assistance Programs. Section 905 requires the Secretary of State to provide a comprehensive annual briefing and periodic updates to Congress on global issues, trends, and actors considered to be significant with respect to cybercrime, the means of enhancing multilateral or bilateral efforts to prevent, investigate, and prosecute cybercrime, and describe U.S. steps to promote the multilateral or bilateral efforts to reach the goals described above. The Secretary of State is also authorized to prioritize foreign assistance programs designed to combat cybercrime in a region or program of significance in order to better combat cybercrime.