

112TH CONGRESS
1ST SESSION

H. R. 174

To enhance homeland security, including domestic preparedness and collective response to terrorism, by amending the Homeland Security Act of 2002 to establish the Cybersecurity Compliance Division and provide authorities to the Department of Homeland Security to enhance the security and resiliency of the Nation's cyber and physical infrastructure against terrorism and other cyber attacks, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

JANUARY 5, 2011

Mr. THOMPSON of Mississippi introduced the following bill; which was referred to the Committee on Homeland Security, and in addition to the Committee on Oversight and Government Reform, for a period to be subsequently determined by the Speaker, in each case for consideration of such provisions as fall within the jurisdiction of the committee concerned

A BILL

To enhance homeland security, including domestic preparedness and collective response to terrorism, by amending the Homeland Security Act of 2002 to establish the Cybersecurity Compliance Division and provide authorities to the Department of Homeland Security to enhance the security and resiliency of the Nation's cyber and physical infrastructure against terrorism and other cyber attacks, and for other purposes.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

1 **SECTION 1. SHORT TITLE.**

2 This Act may be cited as the “Homeland Security
3 Cyber and Physical Infrastructure Protection Act of
4 2011”.

5 **SEC. 2. OFFICE OF CYBERSECURITY AND COMMUNICA-**
6 **TIONS AND CYBERSECURITY COMPLIANCE**
7 **DIVISION.**

8 (a) IN GENERAL.—Subtitle C of title II of the Home-
9 land Security Act of 2002 (6 U.S.C. 141 et seq.) is amend-
10 ed by redesignating sections 221 through 225 in order as
11 section 226 through 229, respectively, and by inserting be-
12 fore section 222 (as so redesignated) the following:

13 **“SEC. 221. DEFINITIONS.**

14 “In this subtitle:

15 “(1) COMMON CRITERIA FOR INFORMATION
16 TECHNOLOGY SECURITY EVALUATION.—The term
17 ‘common criteria for information technology security
18 evaluation’ means international standard for com-
19 puter security codified in the International Organi-
20 zation for Standardization and the International
21 Electrotechnical Commission standard 15408 (ISO/
22 IEC 15408).

23 “(2) COVERED CRITICAL INFRASTRUCTURE.—
24 The term ‘covered critical infrastructure’ means sys-
25 tems and assets designated by the Director under
26 section 224(e).

1 “(3) CYBER INCIDENT.—The term ‘cyber inci-
2 dent’ means an occurrence that jeopardizes the secu-
3 rity of data or the physical security of a computer
4 network owned or operated by a Federal agency or
5 covered critical infrastructure.

6 “(4) FIRST-PARTY REGULATORY AGENCY.—The
7 term ‘first-party regulatory agency’ means a Federal
8 agency that is not a sector-specific agency but that
9 has primary regulatory authority for a specific crit-
10 ical infrastructure sector or sub-sector.

11 “(5) SECTOR-SPECIFIC AGENCY.—The term
12 ‘sector-specific agency’ means the agency that, as of
13 the date of enactment of this section, is designated
14 under Homeland Security Presidential Directive 7 as
15 the lead Federal agency responsible for securing a
16 specific critical infrastructure sector.

17 **“SEC. 222. OFFICE OF CYBERSECURITY AND COMMUNICA-**
18 **TIONS.**

19 “(a) ESTABLISHMENT.—

20 “(1) IN GENERAL.—There shall be in the De-
21 partment an Office of Cybersecurity and Commu-
22 nications.

23 “(2) ASSISTANT SECRETARY FOR CYBERSECUR-
24 ITY AND COMMUNICATIONS.—The Assistant Sec-

1 retary for Cybersecurity and Communications shall
2 be the head of the Office.

3 “(3) COMPONENTS.—The Office shall include—

4 “(A) the United States Computer Emer-
5 gency Readiness Team, as in effect on the date
6 of enactment of this section;

7 “(B) the Cybersecurity Compliance Divi-
8 sion established by subsection (b); and

9 “(C) other components of the Department
10 that have primary responsibilities for emergency
11 or national communications or cybersecurity.

12 “(b) CYBERSECURITY COMPLIANCE DIVISION.—

13 “(1) IN GENERAL.—There is established in the
14 Office of Cybersecurity and Communications a Cy-
15 bersecurity Compliance Division.

16 “(2) DIRECTOR.—The Cybersecurity Compli-
17 ance Division shall be headed by a Director, who
18 shall be appointed by the Secretary or the Sec-
19 retary’s designee from among individuals who pos-
20 sess—

21 “(A) demonstrated knowledge and ability
22 in cybersecurity, information technology, infra-
23 structure protection, and the operation, secu-
24 rity, and resilience of communications networks;

1 “(B) significant executive leadership, regu-
2 latory, and management experience in the pub-
3 lic or private sector; and

4 “(C) other skills or attributes the Sec-
5 retary considers necessary.

6 “(3) DUTIES AND RESPONSIBILITIES.—The Di-
7 rector—

8 “(A) shall issue risk-based, performance-
9 based regulations, after notice and comment, in
10 accordance with section 224;

11 “(B) shall serve as the first-party regu-
12 latory agency to enforce regulations under sec-
13 tion 224 for computer networks and assets in
14 critical infrastructure sectors for which the Of-
15 fice of Cybersecurity and Communications or
16 any of its components is the designated sector-
17 specific agency;

18 “(C) may require a first-party regulatory
19 agency or sector-specific agency to coordinate
20 with the Director to—

21 “(i) develop and publish, for covered
22 critical infrastructure sectors or subsec-
23 tors, risk-based and performance-based
24 regulations after notice and comment in
25 accordance with paragraph (1), with any

1 appropriate modifications, as identified by
2 the Director, necessary for application to a
3 specific critical infrastructure sector or
4 subsector; and

5 “(ii) enforce the regulations promul-
6 gated under paragraph (1); and

7 “(D) may delegate part or all of the re-
8 sponsibilities and authorities for securing pri-
9 vate sector networks under this section to an
10 appropriate first-party regulatory agency or sec-
11 tor-specific agency, which shall report to the Di-
12 rector all activities it carries out pursuant to
13 such delegation.

14 “(4) RESOURCES.—There is authorized to be
15 appropriated such sums as may be necessary for the
16 operations of the Cybersecurity Compliance Division
17 for each of fiscal years 2012, 2013, and 2014.

18 **“SEC. 223. DEPARTMENT RESPONSIBILITIES AND AUTHORI-**
19 **TIES FOR SECURING FEDERAL GOVERNMENT**
20 **NETWORKS.**

21 “(a) IN GENERAL.—The Secretary, acting through
22 the Assistant Secretary for Cybersecurity and Commu-
23 nications or the Director of the Cybersecurity Compliance
24 Division pursuant to subparagraphs (B), (C), and (D) of
25 subsection (b)(2), shall establish and enforce cybersecurity

1 requirements for civilian nonmilitary and nonintelligence
2 community Federal systems to prevent, deter, prepare for,
3 detect, report, attribute, mitigate, respond to, and recover
4 from cyber attacks and other cyber incidents.

5 “(b) INTERAGENCY WORKING GROUP.—

6 “(1) IN GENERAL.—The Assistant Secretary for
7 Cybersecurity and Communications shall establish
8 and chair an interagency working group that shall
9 include, at a minimum, representation of all chief in-
10 formation officers from all Federal civilian agencies,
11 the Director of the Cybersecurity Compliance divi-
12 sion, the Assistant Secretary for Infrastructure Pro-
13 tection, and the White House Cybersecurity Coordi-
14 nator. The Assistant Secretary shall invite the Sec-
15 retary of Defense, the Director of the National Secu-
16 rity Agency, and the Director of National Intel-
17 ligence to participate as nonvoting representatives
18 for purposes of advising the interagency working
19 group.

20 “(2) FUNCTIONS.—The interagency working
21 group shall—

22 “(A) meet at the call of the Chair;

23 “(B) develop and adopt risk-based, per-
24 formance-based cybersecurity requirements for

1 civilian Federal agency computer networks and
2 federally owned critical infrastructure;

3 “(C) develop and adopt a range of rem-
4 edies, including penalties, for noncompliance of
5 the requirements adopted under paragraph (2),
6 each agency having one vote;

7 “(D) develop recommended budgets for se-
8 curity of the civilian nonmilitary and non-intel-
9 ligence community Federal agency computer
10 networks; and

11 “(E) propose updates, as necessary, for the
12 Common Criteria for Information Technology
13 Security Evaluation as part of a supply chain
14 risk management strategy designed to ensure
15 the security and resilience of the Federal infor-
16 mation infrastructure, including protection
17 against unauthorized access to, alteration of in-
18 formation in, disruption of operations of, inter-
19 ruption of communications or services of, and
20 insertion of malicious software, engineering
21 vulnerabilities, or otherwise corrupting soft-
22 ware, hardware, services, or products intended
23 for use in Federal information infrastructure.

24 “(3) ADOPTION BY VOTE.—Adoption of require-
25 ments and remedies under subparagraphs (B) and

1 (C) of paragraph (2) shall be by a majority vote of
2 the members of the interagency working group, in
3 which each agency with a voting representative on
4 the interagency working group has one vote.

5 “(c) CODIFICATION OF AGREEMENTS.—All measures
6 adopted under subsection (b) shall be submitted by the
7 Secretary to the Office of Management and Budget for
8 establishment in a binding Governmentwide memo or cir-
9 cular.

10 “(d) ENFORCEMENT OF CYBERSECURITY REQUIRE-
11 MENTS FOR FEDERAL GOVERNMENT NETWORKS.—The
12 Assistant Secretary, acting through the Director of the
13 Cybersecurity Compliance Division, may enforce all re-
14 quirements adopted under subsection (b)(2)(B).

15 “(e) CERTIFICATIONS, AUDITS, AND INSPECTIONS.—
16 The Director of the Cybersecurity Compliance Division, in
17 carrying out the Assistant Secretary for Cybersecurity and
18 Communications’ enforcement authority under subsection
19 (d), shall require a certification of compliance from the
20 head of each civilian Federal agency that is subject to the
21 requirements under subsection (b)(2)(B), and may con-
22 duct announced or unannounced audits and inspections of
23 any network owned, operated, or used by a Federal civilian
24 agency.

1 “(f) ENFORCEMENT.—If a certification, audit, or in-
2 spection carried out under subsection (e) shows non-
3 compliance with a requirement under subsection
4 (b)(2)(B), Assistant Secretary, acting through the Direc-
5 tor of the Cybersecurity Compliance Division, may identify
6 the appropriate remedies, including penalties, under sub-
7 section (b)(2)(C).

8 “(g) EXECUTION OF PENALTIES BY OMB.—The Di-
9 rector of the Office of Management and Budget shall exe-
10 cute each remedy identified by the Director of the Cyber-
11 security Compliance Division under subsection (f) on be-
12 half of the Assistant Secretary.

13 “(h) REPORTING OF CYBER INCIDENTS ON FEDERAL
14 NETWORKS.—The requirements under subsection
15 (b)(2)(B) shall include a requirement that all Federal enti-
16 ties report any cyber incidents on their computer networks
17 to the Director and to the United States Computer Emer-
18 gency Readiness Team.

19 “(i) RESPONDING TO CYBER INCIDENTS ON FED-
20 ERAL NETWORKS.—If an incident is reported under sub-
21 section (h), the United States Computer Emergency Read-
22 iness Team shall, in coordination with the reporting agen-
23 cy, research the incident to determine and report to the
24 Director and the reporting agency—

25 “(1) the extent of any compromise;

1 “(2) an identification of any attackers, includ-
2 ing any affiliations with terrorists, terrorist organi-
3 zations, criminal organizations, state entities, and
4 nonstate entities;

5 “(3) the method of penetration;

6 “(4) ramifications of any such compromise on
7 future operations;

8 “(5) secondary ramifications of any such com-
9 promise on other Federal or non-Federal networks;

10 “(6) ramifications of any such compromise on
11 national security, including war fighting capability;
12 and

13 “(7) recommended mitigation activities.

14 **“SEC. 224. DEPARTMENT RESPONSIBILITIES AND AUTHORI-**
15 **TIES FOR SECURING PRIVATE SECTOR NET-**
16 **WORKS.**

17 “(a) FINDINGS.—Congress finds that—

18 “(1) pursuant to Homeland Security Presi-
19 dential Directive 7 the Department established pub-
20 lic-private partnerships including Government Co-
21 ordinating Councils (GCCs) and Sector Coordinating
22 Councils (SCCs) to aid in the task of protecting the
23 Nation’s critical infrastructures;

1 “(2) as part of this structure, each critical in-
2 frastructure sector has a designated sector-specific
3 agency;

4 “(3) the designated sector-specific agency for
5 the Information Technology sector is the Office of
6 Cybersecurity and Communications, and the des-
7 ignated sector-specific agency for the communica-
8 tions sector is the National Communications System,
9 which resides within the Office of Cybersecurity and
10 Communications;

11 “(4) if cybersecurity regulation are necessary,
12 the Department, consistent with the entire GCC/
13 SCC structure, as the sector-specific agency, will be
14 the regulator for cybersecurity requirements within
15 the information technology and communications sec-
16 tors; and

17 “(5) in other critical infrastructure sectors, en-
18 forcement of cybersecurity regulations should be ac-
19 complished through appropriate first-party regu-
20 latory agencies or sector-specific agencies.

21 “(b) GENERAL AUTHORITY.—The Secretary, acting
22 through the Director, may establish and enforce risk-
23 based cybersecurity requirements for private sector com-
24 puter networks within covered critical infrastructures.

1 “(c) RISK-BASED CYBERSECURITY REQUIREMENTS
2 FOR CRITICAL INFRASTRUCTURE.—

3 “(1) IN GENERAL.—The Director shall promul-
4 gate risk-based, performance-based cybersecurity re-
5 quirements for covered critical infrastructures, that
6 are designed to prevent, deter, prepare for, detect,
7 report, attribute, mitigate, respond to and recover
8 from cyber incidents.

9 “(2) RISK FACTORS.—The requirements shall
10 be based on the risk factors of threats,
11 vulnerabilities, and consequences, as follows:

12 “(A) THREATS.—The requirements shall
13 be based on terrorist or other known adversary
14 capabilities and intent, or the likelihood of a po-
15 tential terrorist or other adversary attacking or
16 causing a cyber incident against critical infra-
17 structure, as identified by the Secretary in con-
18 sultation with the Director of National Intel-
19 ligence, including—

20 “(i) theft, modification, compromise,
21 damage, or destruction of data or data-
22 bases;

23 “(ii) physical compromise, damage, or
24 destruction of covered critical infrastruc-
25 tures; and

1 “(iii) national, corporate, or personal
2 espionage.

3 “(3) VULNERABILITIES.—The requirements
4 shall require security measures based on—

5 “(A) preparedness;

6 “(B) target attractiveness; and

7 “(C) deterrence capabilities.

8 “(4) CONSEQUENCES.—The requirements shall
9 require security measures based on—

10 “(A) the potential extent and likelihood of
11 death, injury, or serious adverse effects to
12 human health and safety caused by a disruption
13 of the reliable operation of covered critical in-
14 frastructure;

15 “(B) the threat to or potential impact on
16 national security caused by a disruption of the
17 reliable operation of covered critical infrastruc-
18 ture;

19 “(C) the extent to which the disruption of
20 the reliable operation of covered critical infra-
21 structure will disrupt the reliable operation of
22 other covered critical infrastructure;

23 “(D) the potential for harm to the econ-
24 omy that would result from a disruption of the

1 reliable operation of covered critical infrastruc-
2 ture; and

3 “(E) other risk-based security factors that
4 the Director, in consultation with the head of
5 the sector-specific agency that is the first-party
6 regulatory agency with responsibility for the
7 covered critical infrastructure concerned, deter-
8 mines to be appropriate and necessary to pro-
9 tect public health and safety, critical infrastruc-
10 ture, national security, or economic security.

11 “(d) CONSULTATION.—In establishing security per-
12 formance requirements under subsection (c), the Director
13 shall, to the maximum extent practicable, consult with—

14 “(1) the Assistant Secretary for Infrastructure
15 Protection of the Department;

16 “(2) the Officer for Civil Rights and Civil Lib-
17 erties of the Department;

18 “(3) the Chief Privacy Officer of the Depart-
19 ment;

20 “(4) the Under Secretary for Intelligence and
21 Analysis;

22 “(5) the Director of National Intelligence;

23 “(6) the Director of the National Security
24 Agency;

1 “(7) the Director of the National Institute of
2 Standards and Technology;

3 “(8) the heads of sector-specific agencies;

4 “(9) the heads of first-party regulatory agen-
5 cies;

6 “(10) private sector companies or industry
7 groups, including but not limited to members of ap-
8 propriate sector coordinating councils;

9 “(11) State, local, and tribal agency representa-
10 tives;

11 “(12) academic institutions and think tanks;

12 “(13) private sector, government, and nonprofit
13 entities that specialize in privacy and civil liberties;
14 and

15 “(14) the White House Cybersecurity Coordi-
16 nator.

17 “(e) COVERED CRITICAL INFRASTRUCTURES.—

18 “(1) DESIGNATION.—The Director shall—

19 “(A) determine, in consultation with the
20 heads of sector-specific agencies and the heads
21 of first-party regulatory agencies, which sys-
22 tems or assets of critical infrastructure shall be
23 subject to the requirements of this section and
24 designate them as covered critical infrastruc-
25 tures for purposes of this section;

1 “(B) notify each first-party regulatory
2 agency or sector-specific agency of each such
3 determination; and

4 “(C) acting through the corresponding
5 first-party regulatory agency or sector-specific
6 agency, notify owners or operators of covered
7 critical infrastructure sectors of the require-
8 ments of this subtitle.

9 “(2) REQUIREMENTS.—A system or asset may
10 not be designated as covered critical infrastructure
11 under paragraph (1) unless—

12 “(A) the system or asset meets the re-
13 quirements for inclusion on the prioritized crit-
14 ical infrastructure list established by the Sec-
15 retary under section 210E(a)(2);

16 “(B) the system or asset is a component of
17 the national information infrastructure or the
18 national information infrastructure is essential
19 to the reliable operation of the system or asset;
20 or

21 “(C) the destruction or the disruption of
22 the reliable operation of the system or asset
23 would cause a national or regional catastrophe.

24 “(3) FACTORS TO BE CONSIDERED.—In desig-
25 nating systems or assets under this section, the Di-

1 rector shall consider cyber risks and consequences by
2 sector, including—

3 “(A) the factors listed in section subsection
4 (c);

5 “(B) known cyber incidents or cyber risks
6 identified by existing risk assessments;

7 “(C) interdependencies between compo-
8 nents of covered critical infrastructure; and

9 “(D) the potential for the destruction or
10 disruption of the system or asset to cause—

11 “(i) a mass casualty event with an ex-
12 traordinary number of fatalities;

13 “(ii) severe economic consequences;

14 “(iii) mass evacuations with a pro-
15 longed absence; or

16 “(iv) severe degradation of national
17 security capabilities, including intelligence
18 and defense functions.

19 “(4) RECONSIDERATION.—Prior to a final des-
20 ignation of a system or asset of critical infrastruc-
21 ture under this subsection, the Director shall provide
22 the owner or operator of the system or asset an op-
23 portunity to appeal the determination made under
24 paragraph (1)(A).

1 “(f) CYBERSECURITY PLANS.—The Director shall re-
2 quire entities determined under subsection (e) to be cov-
3 ered critical infrastructures to comply with the require-
4 ments under subsection (c) and to submit to the first-
5 party regulatory agency or sector-specific agency, a pro-
6 posed cybersecurity plan to satisfy the security perform-
7 ance requirements described in subsection (c) on a
8 timeline determined by the Director.

9 “(g) CYBERSECURITY PLAN REVIEW.—Upon submis-
10 sion of the plan, the first-party regulatory agency or sec-
11 tor-specific agency shall, based on guidance provided by
12 the Director—

13 “(1) review cybersecurity plans submitted pur-
14 suant to subsection (f);

15 “(2) approve or disapprove each cybersecurity
16 plan;

17 “(3) notify the submitter of the cybersecurity
18 plan of approval or disapproval;

19 “(4) in the case of disapproval, provide a clear
20 explanation of the reasons for disapproval, possible
21 changes that would result in approval, and provide
22 a timetable for resubmission for compliance; and

23 “(5) inform the Director of any approvals or
24 disapprovals.

1 “(h) IMPLEMENTATION OF CYBERSECURITY
2 PLANS.—

3 “(1) IN GENERAL.—The owners and operators
4 of covered critical infrastructure shall have flexibility
5 in their cybersecurity plans to implement any cyber-
6 security measure, or combination thereof, to satisfy
7 the cybersecurity performance requirements de-
8 scribed in subsection (c) and the first-party regu-
9 latory agency or sector-specific agency may not dis-
10 approve under this section any proposed cybersecu-
11 rity measures, or combination thereof, based on the
12 presence or absence of any particular cybersecurity
13 measure if the proposed cybersecurity measures, or
14 combination thereof, satisfy the cybersecurity per-
15 formance requirements established by the Director
16 under subsection (c).

17 “(2) RECOMMENDED CYBERSECURITY MEAS-
18 URES.—The Assistant Secretary for Cybersecurity
19 and Communications may, at the request of an
20 owner and operator of covered critical infrastructure,
21 recommend a specific cybersecurity measure, or com-
22 bination thereof, that will satisfy the cybersecurity
23 performance requirements established by the Direc-
24 tor. The absence of the recommended security meas-
25 ures, or combination thereof, may not serve as the

1 basis for a disapproval of the security measure, or
2 combination thereof, proposed by the owner or oper-
3 ator of covered critical infrastructure if the proposed
4 security measure, or combination thereof, otherwise
5 satisfies the security performance requirements es-
6 tablished by the Director under (c).

7 “(i) ENFORCEMENT CERTIFICATIONS, AUDITS AND
8 INSPECTIONS.—The sector-specific agency or first-party
9 regulatory agency, in enforcing the requirements under
10 subsection (c), shall require an entity with a cybersecurity
11 plan approved under subsection (g) to certify that the cy-
12 bersecurity plan has been implemented, and may conduct
13 announced or unannounced audits and inspections of any
14 such entity to determine compliance.

15 “(j) REPORTING OF CYBER INCIDENTS ON COVERED
16 CRITICAL INFRASTRUCTURE NETWORKS.—The require-
17 ments under subsection (c) shall include a requirement
18 that each covered critical infrastructure entity report any
19 cyber incidents on its networks to the first-party regu-
20 latory agency for the entity or to the sector-specific agency
21 for the entity (if there is no first-party regulatory agency),
22 and to US CERT.

23 “(k) RESPONDING TO CYBER INCIDENTS ON PRI-
24 VATE NETWORKS.—If an incident is reported under sub-
25 section (j), the United States Computer Emergency Readi-

1 ness Team may, at the invitation of and in coordination
2 with the reporting entity, investigate the incident to deter-
3 mine and report to the Director and the reporting entity—

4 “(1) the extent of any compromise;

5 “(2) an identification of any attackers, includ-
6 ing any affiliations with terrorists, terrorist organi-
7 zations, state entities, and nonstate entities;

8 “(3) the method of penetration;

9 “(4) ramifications of any such compromise on
10 future operations;

11 “(5) secondary ramifications of any such com-
12 promise on other Federal or non-Federal networks;

13 “(6) ramifications of any such compromise on
14 national security, including war fighting capability;
15 and

16 “(7) recommended mitigation activities.

17 “(1) SAFETY ACT INCENTIVES.—The Director may
18 recommend SAFETY Act designation and certification to
19 entities determined under subsections (g) and (i) to be in
20 compliance with the requirements of this section.

21 “(m) PENALTIES.—In the case of noncompliance
22 with the requirements of this section the Director may rec-
23 ommend rescission or suspension of SAFETY Act designa-
24 tion and certification during the period of noncompliance,

1 and may levy civil penalties, not to exceed \$100,000 per
2 day, for each instance of noncompliance.”.

3 (b) DEADLINES.—The Cybersecurity Compliance Di-
4 vision of the Department of Homeland Security shall—

5 (1) not later than six months after such date of
6 enactment of this Act, publish a notice of proposed
7 rulemaking for regulations required under section
8 224 of the Homeland Security Act of 2002, as
9 amended by this section; and

10 (2) not later than one year after such date of
11 enactment of this Act, promulgate final regulations
12 required under such section.

13 (c) RULE OF CONSTRUCTION.—Nothing in this sec-
14 tion shall be construed to provide authority to any sector-
15 specific agency or first-party regulatory agency to estab-
16 lish standards or other measures outside of the require-
17 ments of this Act except as required by this Act and the
18 amendments made by this Act.

19 (d) CLERICAL AMENDMENT.—The table of contents
20 in section 1(b) of such Act is amended by striking the
21 items relating to sections 221 through 225 and inserting
22 the following:

“Sec. 221. Definitions.

“Sec. 222. Office of Cybersecurity and Communications.

“Sec. 223. Department responsibilities and authorities for securing Federal
Government networks.

“Sec. 224. Department responsibilities and authorities for securing private sec-
tor networks.

“Sec. 225. Procedures for sharing information.

“Sec. 226. Privacy Officer.

“Sec. 227. Enhancement of non-Federal cybersecurity.

“Sec. 228. Net guard.

“Sec. 229. Cyber Security Enhancement Act of 2002.”.

1 **SEC. 3. INFORMATION SHARING.**

2 The Assistant Secretary for Cybersecurity and Com-
3 munications of the Department of Homeland Security in
4 coordination with the Assistant Secretary Infrastructure
5 Protection of the Department of Homeland Security shall,
6 to the maximum extent possible, consistent with rules for
7 the handling of classified information, share relevant in-
8 formation regarding cybersecurity threats and
9 vulnerabilities, and any proposed actions to mitigate them,
10 with all Federal agencies, appropriate State, local, or trib-
11 al authority representatives, and all covered critical infra-
12 structure owners and operators, including by expediting
13 necessary security clearances for designated points of con-
14 tact for critical infrastructures.

15 **SEC. 4. INFORMATION PROTECTION.**

16 The Assistant Secretary for Cybersecurity and Com-
17 munications of the Department of Homeland Security
18 shall designate, as appropriate, information received from
19 Federal agencies pursuant to the requirements enacted by
20 section 2 (including the amendments made by such sec-
21 tion), information received from covered critical infra-
22 structure owners and operators pursuant to such section,
23 and information provided to Federal agencies or covered

1 critical infrastructure owners and operators pursuant to
2 this section as sensitive security information and shall re-
3 quire and enforce sensitive security information require-
4 ments for handling, storage, and dissemination of any
5 such information.

6 **SEC. 5. CYBERSECURITY RESEARCH AND DEVELOPMENT.**

7 (a) IN GENERAL.—The Under Secretary for Science
8 and Technology of the Department of Homeland Security
9 shall support research, development, testing, evaluation,
10 and transition of cybersecurity technology, including fun-
11 damental, long-term research to improve the ability of the
12 United States to prevent, protect against, detect, respond
13 to, and recover from acts of terrorism and cyber attacks,
14 with an emphasis on research and development relevant
15 to large-scale, high-impact attacks.

16 (b) ACTIVITIES.—The research and development sup-
17 ported under subsection (a) shall include work to—

18 (1) advance the development and accelerate the
19 deployment of more secure versions of fundamental
20 Internet protocols and architectures, including for
21 the domain name system and routing protocols;

22 (2) improve and create technologies for detect-
23 ing attacks or intrusions, including real-time moni-
24 toring and real-time analytic technologies;

1 (3) improve and create mitigation and recovery
2 methodologies, including techniques and policies for
3 real-time containment of attacks, and development
4 of resilient networks and systems that degrade
5 gracefully;

6 (4) develop and support infrastructure and tools
7 to support cybersecurity research and development
8 efforts, including modeling, test beds, and data sets
9 for assessment of new cybersecurity technologies;

10 (5) assist the development and support of tech-
11 nologies to reduce vulnerabilities in process control
12 systems;

13 (6) develop and support cyber forensics and at-
14 tack attribution; and

15 (7) test, evaluate, and facilitate the transfer of
16 technologies associated with the engineering of less
17 vulnerable software and securing the information
18 technology software development lifecycle.

19 (c) COORDINATION.—In carrying out this section, the
20 Under Secretary shall coordinate activities with—

21 (1) the Under Secretary for National Protection
22 and Programs, the Assistant Secretary for Cyberse-
23 curity and Communications, and the Assistant Sec-
24 retary for Infrastructure Protection of the Depart-
25 ment of Homeland Security; and

1 (2) the heads of other relevant Federal depart-
2 ments and agencies, including the National Science
3 Foundation, the Defense Advanced Research
4 Projects Agency, the Information Assurance Direc-
5 torate of the National Security Agency, the National
6 Institute of Standards and Technology, the Depart-
7 ment of Commerce, and other appropriate working
8 groups established by the President to identify
9 unmet needs and cooperatively support activities, as
10 appropriate.

11 **SEC. 6. CYBER WORKFORCE RECRUITMENT, DEVELOP-**
12 **MENT, AND RETENTION.**

13 (a) WORKFORCE PLAN.—Not later than 180 days
14 after the date of enactment of this Act and in every subse-
15 quent year, the Assistant Secretary for Cybersecurity and
16 Communication of the Department of Homeland Security
17 shall develop a strategic cybersecurity workforce plan as
18 part of the Federal agency performance plan required
19 under section 1115 of title 31, United States Code, that
20 includes—

21 (1) a description of the Department’s cyberse-
22 curity mission; and

23 (2) a description and analysis, relating to the
24 specialized workforce needed by the Department to

1 fulfill the Federal agency's cybersecurity mission, in-
2 cluding—

3 (A) the cybersecurity workforce needs of
4 the Department on the date of the report, and
5 near-, mid-, and long-term projections of work-
6 force needs;

7 (B) hiring projections to meet cybersecu-
8 rity workforce needs, including, for at least a 2-
9 year period, specific occupation and grade lev-
10 els;

11 (C) long-term and short-term strategic
12 goals to address critical skills deficiencies, in-
13 cluding analysis of the numbers of and reasons
14 for attrition of employees;

15 (D) recruitment strategies to attract highly
16 qualified candidates from diverse backgrounds
17 and geographic locations;

18 (E) an assessment of the sources and
19 availability of individuals with needed expertise;

20 (F) ways to streamline the hiring process;

21 (G) the barriers to recruiting and hiring
22 individuals qualified in cybersecurity and rec-
23 ommendations to overcome the barriers; and

24 (H) a training and development plan to en-
25 hance and improve the knowledge of employees.

1 (b) TRAINING.—

2 (1) FEDERAL GOVERNMENT EMPLOYEES AND
3 FEDERAL CONTRACTORS.—The Assistant Secretary
4 for Cybersecurity and Communications shall estab-
5 lish a cybersecurity awareness and education cur-
6 riculum that shall be required for all Federal em-
7 ployees and contractors engaged in the design, devel-
8 opment, or operation of civilian Federal agency com-
9 puter networks.

10 (2) CONTENTS.—The curriculum established
11 under paragraph (1) may include—

12 (A) role-based security awareness training;

13 (B) recommended cybersecurity practices;

14 (C) cybersecurity recommendations for
15 traveling abroad;

16 (D) unclassified counterintelligence infor-
17 mation;

18 (E) information regarding industrial espio-
19 nage;

20 (F) information regarding malicious activ-
21 ity online;

22 (G) information regarding cybersecurity
23 and law enforcement;

24 (H) identity management information;

1 (I) information regarding supply chain se-
2 curity;

3 (J) information security risks associated
4 with the activities of Federal employees; and

5 (K) the responsibilities of Federal employ-
6 ees in complying with policies and procedures
7 designed to reduce information security risks
8 identified under subparagraph (J).

9 (c) EDUCATION OPPORTUNITIES.—The Assistant
10 Secretary for Cybersecurity and Communications shall de-
11 velop and implement a strategy to provide Federal employ-
12 ees who work in cybersecurity-related areas with the op-
13 portunity to obtain additional education.

14 (d) DIRECT HIRE AUTHORITY.—Without regard to
15 the civil service laws (other than sections 3303 and 3328
16 of title 5, United States Code), the Secretary, acting
17 through the Assistant Secretary for Cybersecurity and
18 Communications, in consultation with the Under Sec-
19 retary for Management, may appoint not more than 500
20 employees under this subsection to carry out the require-
21 ments of this Act at a rate of pay that may not exceed
22 the maximum rate of basic pay payable under section
23 5376 of title 5, United States Code, upon certification to
24 the Congress that standard Federal hiring processes have

1 not resulted in the required number of critical cybersecu-
2 rity positions being filled.

3 (e) RETENTION BONUSES.—Notwithstanding section
4 5754 of title 5, United States Code, the Director may pay
5 a retention bonus under that section to any individual ap-
6 pointed under this section, if the Secretary, acting through
7 Assistant Secretary for Cybersecurity and Communica-
8 tions, in consultation with the Under Secretary for Man-
9 agement, determines that, in the absence of a retention
10 bonus, there is a high risk that the individual would likely
11 leave employment with the Department. The Secretary
12 shall submit a written explanation of this determination
13 to Congress prior to announcing the use of this authority.

○