

108TH CONGRESS
2D SESSION

H. R. 5068

To amend the Homeland Security Act of 2002 to enhance cybersecurity,
and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

SEPTEMBER 13, 2004

Mr. THORNBERRY (for himself and Ms. LOFGREN) introduced the following bill; which was referred to the Select Committee on Homeland Security, and in addition to the Committee on Science, 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 amend the Homeland Security Act of 2002 to enhance
cybersecurity, 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,*

3 **SECTION 1. SHORT TITLE.**

4 This Act may be cited as the “Department of Home-
5 land Security Cybersecurity Enhancement Act of 2004”.

6 **SEC. 2. ASSISTANT SECRETARY FOR CYBERSECURITY.**

7 (a) IN GENERAL.—Subtitle A of title II of the Home-
8 land Security Act of 2002 (6 U.S.C. 121 et seq.) is amend-
9 ed by adding at the end the following:

1 **“SEC. 203. ASSISTANT SECRETARY FOR CYBERSECURITY.**

2 “(a) IN GENERAL.—There shall be in the Directorate
3 for Information Analysis and Infrastructure Protection a
4 National Cybersecurity Office headed by an Assistant Sec-
5 retary for Cybersecurity (in this section referred to as the
6 ‘Assistant Secretary’), who shall assist the Secretary in
7 promoting cybersecurity for the Nation.

8 “(b) GENERAL AUTHORITY.—The Assistant Sec-
9 retary, subject to the direction and control of the Sec-
10 retary, shall have primary authority within the Depart-
11 ment for all cybersecurity-related critical infrastructure
12 protection programs of the Department, including with re-
13 spect to policy formulation and program management.

14 “(c) RESPONSIBILITIES.—The responsibilities of the
15 Assistant Secretary shall include the following:

16 “(1) To establish and manage—

17 “(A) a national cybersecurity response sys-
18 tem that includes the ability to—

19 “(i) analyze the effect of cybersecurity
20 threat information on national critical in-
21 frastructure; and

22 “(ii) aid in the detection and warning
23 of attacks on, and in the restoration of,
24 cybersecurity infrastructure in the after-
25 math of such attacks;

1 “(B) a national cybersecurity threat and
2 vulnerability reduction program that identifies
3 cybersecurity vulnerabilities that would have a
4 national effect on critical infrastructure, per-
5 forms vulnerability assessments on information
6 technologies, and coordinates the mitigation of
7 such vulnerabilities;

8 “(C) a national cybersecurity awareness
9 and training program that promotes
10 cybersecurity awareness among the public and
11 the private sectors and promotes cybersecurity
12 training and education programs;

13 “(D) a government cybersecurity program
14 to coordinate and consult with Federal, State,
15 and local governments to enhance their
16 cybersecurity programs; and

17 “(E) a national security and international
18 cybersecurity cooperation program to help fos-
19 ter Federal efforts to enhance international
20 cybersecurity awareness and cooperation.

21 “(2) To coordinate with the private sector on
22 the program under paragraph (1) as appropriate,
23 and to promote cybersecurity information sharing,
24 vulnerability assessment, and threat warning regard-
25 ing critical infrastructure.

1 “(3) To coordinate with other directorates and
2 offices within the Department on the cybersecurity
3 aspects of their missions.

4 “(4) To coordinate with the Under Secretary
5 for Emergency Preparedness and Response to en-
6 sure that the National Response Plan developed pur-
7 suant to section 502(6) of the Homeland Security
8 Act of 2002 (6 U.S.C. 312(6)) includes appropriate
9 measures for the recovery of the cybersecurity ele-
10 ments of critical infrastructure.

11 “(5) To develop processes for information shar-
12 ing with the private sector, consistent with section
13 214, that—

14 “(A) promote voluntary cybersecurity best
15 practices, standards, and benchmarks that are
16 responsive to rapid technology changes and to
17 the security needs of critical infrastructure; and

18 “(B) consider roles of Federal, State, local,
19 and foreign governments and the private sector,
20 including the insurance industry and auditors.

21 “(6) To coordinate with the Chief Information
22 Officer of the Department in establishing a secure
23 information sharing architecture and information
24 sharing processes, including with respect to the De-
25 partment’s operation centers.

1 “(7) To consult with the Electronic Crimes
2 Task Force of the United States Secret Service on
3 private sector outreach and information activities.

4 “(8) To consult with the Office for Domestic
5 Preparedness to ensure that realistic cybersecurity
6 scenarios are incorporated into tabletop and recovery
7 exercises.

8 “(9) To consult and coordinate, as appropriate,
9 with other Federal agencies on cybersecurity-related
10 programs, policies, and operations.

11 “(10) To consult and coordinate within the De-
12 partment and, where appropriate, with other rel-
13 evant Federal agencies, on security of digital control
14 systems, such as Supervisory Control and Data Ac-
15 quisition (SCADA) systems.

16 “(d) AUTHORITY OVER THE NATIONAL COMMUNICA-
17 TIONS SYSTEM.—The Assistant Secretary shall have pri-
18 mary authority within the Department over the National
19 Communications System.”.

20 (b) CLERICAL AMENDMENT.—The table of contents
21 in section 1(b) of such Act is amended by adding at the
22 end of the items relating to subtitle A of title II the fol-
23 lowing:

“203. Assistant Secretary for Cybersecurity.”.

1 **SEC. 3. CYBERSECURITY DEFINED.**

2 Section 2 of the Homeland Security Act of 2002 (6
3 U.S.C. 101) is amended by adding at the end the fol-
4 lowing:

5 “(17)(A) The term ‘cybersecurity’ means the
6 prevention of damage to, the protection of, and the
7 restoration of computers, electronic communications
8 systems, electronic communication services, wire
9 communication, and electronic communication, in-
10 cluding information contained therein, to ensure its
11 availability, integrity, authentication, confidentiality,
12 and nonrepudiation.

13 “(B) In this paragraph—

14 “(i) each of the terms ‘damage’ and ‘com-
15 puter’ has the meaning that term has in section
16 1030 of title 18, United States Code; and

17 “(ii) each of the terms ‘electronic commu-
18 nications system’, ‘electronic communication
19 service’, ‘wire communication’, and ‘electronic
20 communication’ has the meaning that term has
21 in section 2510 of title 18, United States
22 Code.”.

○