

110<sup>TH</sup> CONGRESS  
2<sup>D</sup> SESSION

# H. R. 5983

---

IN THE SENATE OF THE UNITED STATES

JULY 31, 2008

Received; read twice and referred to the Committee on Homeland Security and  
Governmental Affairs

---

## AN ACT

To amend the Homeland Security Act of 2002 to enhance  
the information security of the Department of Homeland  
Security, 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 Network Defense and Accountability Act of 2008”.

4 **SEC. 2. AUTHORITY OF CHIEF INFORMATION OFFICER;  
5 QUALIFICATIONS FOR APPOINTMENT.**

6 Section 703(a) of the Homeland Security Act of 2002  
7 (6 U.S.C. 343(a)) is amended—

8 (1) by inserting before the first sentence the  
9 following:

10 “(1) **AUTHORITIES AND DUTIES.**—The Sec-  
11 retary shall delegate to the Chief Information Offi-  
12 cer such authority necessary for the development,  
13 approval, implementation, integration, and oversight  
14 of policies, procedures, processes, activities, funding,  
15 and systems of the Department relating to the man-  
16 agement of information and information infrastruc-  
17 ture for the Department, including the management  
18 of all related mission applications, information re-  
19 sources, and personnel.

20 “(2) **LINE AUTHORITY.**—”; and

21 (2) by adding at the end the following new  
22 paragraphs:

23 “(3) **QUALIFICATIONS FOR APPOINTMENT.**—An  
24 individual may not be appointed as Chief Informa-  
25 tion Officer unless the individual has—

1           “(A) demonstrated ability in and knowl-  
2           edge of information technology and information  
3           security; and

4           “(B) not less than 5 years of executive  
5           leadership and management experience in infor-  
6           mation technology and information security in  
7           the public or private sector.

8           “(4) FUNCTIONS.—The Chief Information Offi-  
9           cer shall—

10           “(A) establish and maintain an incident re-  
11           sponse team that provides a continuous, real-  
12           time capability within the Department of  
13           Homeland Security to—

14           “(i) detect, respond to, contain, inves-  
15           tigate, attribute, and mitigate any com-  
16           puter incident, as defined by the National  
17           Institute of Standards and Technology,  
18           that could violate or pose an imminent  
19           threat of violation of computer security  
20           policies, acceptable use policies, or stand-  
21           ard security practices of the Department;  
22           and

23           “(ii) deliver timely notice of any inci-  
24           dent to individuals responsible for informa-  
25           tion infrastructure of the Department, and

1 to the United States Computer Emergency  
2 Readiness Team;

3 “(B) establish, maintain, and update a  
4 network architecture, including a diagram de-  
5 tailing how security controls are positioned  
6 throughout the information infrastructure of  
7 the Department to maintain the confidentiality,  
8 integrity, availability, accountability, and assur-  
9 ance of electronic information; and

10 “(C) ensure that vulnerability assessments  
11 are conducted on a regular basis for any De-  
12 partment information infrastructure connected  
13 to the Internet or another external network,  
14 and that vulnerabilities are mitigated in a time-  
15 ly fashion.”.

16 **SEC. 3. ATTACK-BASED TESTING PROTOCOLS.**

17 Section 703 of the Homeland Security Act of 2002  
18 (6 U.S.C. 343) is amended by adding at the end the fol-  
19 lowing new subsection:

20 “(c) **ATTACK-BASED TESTING PROTOCOLS.**—The  
21 Chief Information Officer, in consultation with the Inspec-  
22 tor General, the Assistant Secretary for Cybersecurity,  
23 and the heads of other appropriate Federal agencies,  
24 shall—

1           “(1) establish security control testing protocols  
2           that ensure that the Department’s information in-  
3           frastructure is effectively protected against known  
4           attacks against and exploitations of Federal and  
5           contractor information infrastructure;

6           “(2) oversee the deployment of such protocols  
7           throughout the information infrastructure of the De-  
8           partment; and

9           “(3) update such protocols on a regular basis.”.

10 **SEC. 4. INSPECTOR GENERAL REVIEWS OF INFORMATION**  
11 **INFRASTRUCTURE.**

12           Section 703 of the Homeland Security Act of 2002  
13 (6 U.S.C. 343) is further amended by adding at the end  
14 the following new subsection:

15           “(d) INSPECTOR GENERAL REVIEWS.—

16           “(1) IN GENERAL.—The Inspector General of  
17           the Department shall use authority under the In-  
18           spector General Act of 1978 (5 App. U.S.C.) to con-  
19           duct announced and unannounced performance re-  
20           views and programmatic reviews of the information  
21           infrastructure of the Department to determine the  
22           effectiveness of security policies and controls of the  
23           Department.

24           “(2) PERFORMANCE REVIEWS.—Performance  
25           reviews under this subsection shall test and validate

1 a system’s security controls using the protocols cre-  
2 ated under subsection (c), beginning not later than  
3 270 days after the date of enactment of the Home-  
4 land Security Network Defense and Accountability  
5 Act of 2008.

6 “(3) PROGRAMMATIC REVIEWS.—Programmatic  
7 reviews under this subsection shall—

8 “(A) determine whether an agency of the  
9 Department is complying with policies, proc-  
10 esses, and procedures established by the Chief  
11 Information Officer; and

12 “(B) focus on risk assessment, risk man-  
13 agement, and risk mitigation, with primary re-  
14 gard to the implementation of best practices  
15 such as authentication, access control (including  
16 remote access), intrusion detection and preven-  
17 tion, data protection and integrity, and any  
18 other controls that the Inspector General con-  
19 siders necessary.

20 “(4) INFORMATION SECURITY REPORT.—The  
21 Inspector General shall submit a security report con-  
22 taining the results of each review under this sub-  
23 section and prioritized recommendations for improv-  
24 ing security controls based on that review, including

1 recommendations regarding funding changes and  
2 personnel management, to—

3 “(A) the Secretary;

4 “(B) the Chief Information Officer; and

5 “(C) the head of the Department compo-  
6 nent that was the subject of the review, and  
7 other appropriate individuals responsible for the  
8 information infrastructure of such agency.

9 “(5) CORRECTIVE ACTION REPORT.—

10 “(A) IN GENERAL.—Within 60 days after  
11 receiving a security report under paragraph (4),  
12 the head of the Department component that  
13 was the subject of the review and the Chief In-  
14 formation Officer shall jointly submit a correc-  
15 tive action report to the Secretary and the In-  
16 spector General.

17 “(B) CONTENTS.—The corrective action  
18 report—

19 “(i) shall contain a plan for address-  
20 ing recommendations and mitigating  
21 vulnerabilities contained in the security re-  
22 port, including a timeline and budget for  
23 implementing such plan; and

24 “(ii) shall note any matters in dis-  
25 agreement between the head of the Depart-

1                   ment component and the Chief Information  
2                   Officer.

3                   “(6) REPORTS TO CONGRESS.—

4                   “(A) ANNUAL REPORTS.—In conjunction  
5                   with the reporting requirements of section 3545  
6                   of title 44, United States Code, the Inspector  
7                   General shall submit an annual report to the  
8                   Committee on Homeland Security of the House  
9                   of Representatives and the Committee on  
10                  Homeland Security and Governmental Affairs  
11                  of the Senate—

12                  “(i) summarizing the performance and  
13                  programmatic reviews performed during  
14                  the preceding fiscal year, the results of  
15                  those reviews, and any actions that remain  
16                  to be taken under plans included in correc-  
17                  tive action reports under paragraph (5);  
18                  and

19                  “(ii) describing the effectiveness of  
20                  the testing protocols developed under sub-  
21                  section (c) in reducing successful exploi-  
22                  tations of the Department’s information  
23                  infrastructure.

24                  “(B) SECURITY REPORTS AND CORREC-  
25                  TIVE ACTION REPORTS.—The Inspector General

1 shall make all security reports and corrective  
2 action reports available to any member of the  
3 Committee on Homeland Security of the House  
4 of Representatives, any member of the Com-  
5 mittee on Homeland Security and Govern-  
6 mental Affairs of the Senate, and the Comp-  
7 troller General of the United States, upon re-  
8 quest.”.

9 **SEC. 5. INFORMATION INFRASTRUCTURE DEFINED.**

10 Section 703 of the Homeland Security Act of 2002  
11 (6 U.S.C. 343) is further amended by adding at the end  
12 the following:

13 “(e) INFORMATION INFRASTRUCTURE DEFINED.—In  
14 this section, the term ‘information infrastructure’ means  
15 systems and assets used in processing, transmitting, re-  
16 ceiving, or storing information electronically.”.

17 **SEC. 6. NETWORK SERVICE PROVIDERS.**

18 (a) IN GENERAL.—Subtitle D of title VIII of the  
19 Homeland Security Act of 2002 (6 U.S.C. 391 et seq.)  
20 is amended by adding at the end the following new section:

21 **“SEC. 836. REQUIREMENTS FOR NETWORK SERVICE PRO-  
22 VIDERS.**

23 “(a) COMPATIBILITY DETERMINATION.—Before en-  
24 tering into or renewing a covered contract, the Secretary,  
25 acting through the Chief Information Officer, must deter-

1 mine that the contractor has an internal information sys-  
2 tems security policy that complies with the Department’s  
3 information security requirements for risk assessment,  
4 risk management, and risk mitigation, with primary re-  
5 gard to the implementation of best practices such as au-  
6 thentication, access control (including remote access), in-  
7 trusion detection and prevention, data protection and in-  
8 tegrity, and any other policies that the Secretary considers  
9 necessary to ensure the security of the Department’s in-  
10 formation infrastructure.

11 “(b) CONTRACT REQUIREMENTS REGARDING SECUR-  
12 ITY.—The Secretary shall include in each covered con-  
13 tract provisions requiring the contractor to—

14 “(1) implement and regularly update the inter-  
15 nal information systems security policy required  
16 under subsection (a);

17 “(2) maintain the capability to provide con-  
18 tracted services on a continuing and ongoing basis  
19 to the Department in the event of unplanned or dis-  
20 ruptive event; and

21 “(3) deliver timely notice of any internal com-  
22 puter incident, as defined by the National Institute  
23 of Standards and Technology, that could violate or  
24 pose an imminent threat of violation of computer se-  
25 curity policies, acceptable use policies, or standard

1 security practices at the Department, to the United  
2 States Computer Emergency Readiness Team and  
3 the incident response team established under section  
4 703(a)(4).

5 “(c) CONTRACT REQUIREMENTS REGARDING SUB-  
6 CONTRACTING.—The Secretary shall include in each cov-  
7 ered contract—

8 “(1) a requirement that the contractor develop  
9 and implement a plan for the award of subcontracts,  
10 as appropriate, to small business concerns and dis-  
11 advantaged business concerns in accordance with  
12 other applicable requirements, including the terms of  
13 such plan, as appropriate; and

14 “(2) a requirement that the contractor submit  
15 to the Secretary, during performance of the con-  
16 tract, periodic reports describing the extent to which  
17 the contractor has complied with such plan, includ-  
18 ing specification (by total dollar amount and by per-  
19 centage of the total dollar value of the contract) of  
20 the value of subcontracts awarded at all tiers of sub-  
21 contracting to small business concerns, including so-  
22 cially and economically disadvantaged small busi-  
23 nesses concerns, small business concerns owned and  
24 controlled by service-disabled veterans, HUBZone  
25 small business concerns, small business concerns eli-

1       gible to be awarded contracts pursuant to section  
2       8(a) of the Small Business Act (15 U.S.C. 637(a)),  
3       and Historically Black Colleges and Universities and  
4       Hispanic-serving institutions, tribal colleges and uni-  
5       versities, and other minority institutions.

6       “(d) EXISTING CONTRACTS.—The Secretary shall, to  
7       the extent practicable under the terms of existing con-  
8       tracts, require each contractor who provides covered infor-  
9       mation services under a contract in effect on the date of  
10      the enactment of the Homeland Security Network Defense  
11      and Accountability Act of 2008 to comply with the re-  
12      quirements described in subsection (b).

13      “(e) DEFINITIONS.—For purposes of this section:

14           “(1) SOCIALLY AND ECONOMICALLY DISADVAN-  
15      TAGED SMALL BUSINESSES CONCERN, SMALL BUSI-  
16      NESS CONCERN OWNED AND CONTROLLED BY SERV-  
17      ICE-DISABLED VETERANS, AND HUBZONE SMALL  
18      BUSINESS CONCERN.—The terms ‘socially and eco-  
19      nomically disadvantaged small businesses concern’,  
20      ‘small business concern owned and controlled by  
21      service-disabled veterans’, and ‘HUBZone small  
22      business concern’ have the meanings given such  
23      terms under the Small Business Act (15 U.S.C. 631  
24      et seq.).

1           “(2) CONTRACTOR.—The term ‘contractor’ in-  
2           cludes each subcontractor of a contractor.

3           “(3) COVERED CONTRACT.—The term ‘covered  
4           contract’ means a contract entered into or renewed  
5           after the date of the enactment of the Homeland Se-  
6           curity Network Defense and Accountability Act of  
7           2008 for the provision of covered information serv-  
8           ices.

9           “(4) COVERED INFORMATION SERVICES.—The  
10          term ‘covered information services’ means creation,  
11          management, maintenance, control, or operation of  
12          information networks or Internet Web sites for the  
13          Department.

14          “(5) HISTORICALLY BLACK COLLEGES AND  
15          UNIVERSITIES.—The term ‘Historically Black Col-  
16          leges and Universities’ means part B institutions  
17          under title III of the Higher Education Act of 1965  
18          (20 U.S.C. 1061).

19          “(6) HISPANIC-SERVING INSTITUTION.—The  
20          term ‘Hispanic-serving institution’ has the meaning  
21          given such term under title V of the Higher Edu-  
22          cation Act of 1965 (20 U.S.C. 1101a(a)(5)).

23          “(7) INFORMATION INFRASTRUCTURE.—The  
24          term ‘information infrastructure’ has the meaning  
25          that term has under section 703.

1           “(8) TRIBAL COLLEGES AND UNIVERSITIES.—  
2           The term ‘tribal colleges and universities’ has the  
3           meaning given such term under the Tribally Con-  
4           trolled College or University Assistance Act of 1978  
5           (25 U.S.C. 1801 et seq.).”.

6           (b) CLERICAL AMENDMENT.—The table of contents  
7           in section 1(b) of such Act is amended by inserting after  
8           the item relating to section 835 the following new item:  
          “Sec. 836. Requirements for network service providers.”.

9           (c) REPORT.—Within 90 days after the date of enact-  
10          ment of this Act, the Secretary of Homeland Security shall  
11          transmit to the Committee on Homeland Security of the  
12          House of Representatives and the Homeland Security and  
13          Governmental Affairs Committee of the Senate a report  
14          describing—

15               (1) the progress in implementing requirements  
16               issued by the Office of Management and Budget for  
17               encryption, authentication, Internet Protocol version  
18               6, and Trusted Internet Connections, including a  
19               timeline for completion;

20               (2) a plan, including an estimated budget and  
21               a timeline, to investigate breaches against the De-  
22               partment of Homeland Security’s information infra-  
23               structure for purposes of counterintelligence assess-  
24               ment, attribution, and response;

