



H.R. 5983 – Homeland Security Network Defense and Accountability Act of 2008

FLOOR SITUATION

H.R. 5983 is being considered on the floor under suspension of the rules and will require a two-thirds majority vote for passage. This legislation was introduced by Representative James Langevin (D-RI) on May 7, 2008. The House Committee on Homeland Security ordered the bill to be reported, as amended, by voice vote on June 26, 2008.

H.R. 5983 is expected to be considered on the floor of the House on July 29, 2008.

SUMMARY

CIO Authorities: H.R. 5983 amends the Homeland Security Act of 2002 to direct the Secretary of the Department of Homeland Security (DHS) to delegate authority to DHS' Chief Information Officer (CIO) for the development, approval, implementation, integration, and oversight of DHS policies and activities relating to information management and information infrastructure.

CIO Qualifications and Responsibilities: This bill lists certain qualifications for the CIO position, including at least five years of executive leadership and management experience in IT security and also several functions, including establishing an incident response team.

Testing Protocols: H.R. 5983 directs the CIO to establish and regularly update security control testing protocols that ensure that DHS' information infrastructure is effectively protected against known attacks and exploitations.

Reviews: This legislation requires the DHS Inspector General to conduct unannounced performance and programmatic reviews of DHS' information infrastructure to determine the effectiveness of its security policies and controls. The IG must also report annually to Congress regarding these reviews.

Contracting: H.R. 5983 directs the Secretary, before entering or renewing a contract to determine that the contractor has an internal information systems security policy that complies with DHS information security requirements. The Secretary must additionally include a requirement in each contract for the contractor to develop and implement a plan to award appropriate subcontracts to small and disadvantaged businesses.

BACKGROUND

The security of federal and critical infrastructure networks is a significant national security issue. The United States faces a growing threat to its information technology (IT) systems and assets, and to the integrity of information. For example, recently Reps. Frank Wolf (R-VA) and Chris Smith (R-NJ) disclosed that their office staffs' computers had been targeted by Chinese hackers.

Although Federal agencies have shown improvement recently in the cyber security arena, they have continued to score low grades in the annual report on their compliance with the Federal Information Security Management Act (FISMA) of 2002. Most federal agencies lag behind an aggressive timetable for switching over all government desktop systems to a set of standard configurations designed to increase security. Currently, DHS operates a National Cyber Security Division (NCSD) which works collaboratively with public, private and international entities to secure cyberspace and our Nation's cyber assets

COST



LEGISLATIVE DIGEST

HOUSE REPUBLICAN CONFERENCE | CHAIRMAN ADAM PUTNAM

1420 LONGWORTH HOB, WASHINGTON, DC 20515

www.GOP.gov

PHONE 202.225.5107

FAX 202.226.0154

The Congressional Budget Office (CBO) estimates that implementing H.R. 5983 “would cost \$163 million over the 2009-2013 period for DHS to hire additional staff to carry out the bill’s provisions.” [Full CBO Cost Estimate](#)

STAFF CONTACT

For questions or further information contact Adam Hepburn at (202) 226-2302.