106TH CONGRESS
2D SESSION

S. 2702

To require reports on the progress of the Federal Government in implementing Presidential Decision Directive No. 63 (PDD–63).

IN THE SENATE OF THE UNITED STATES

JUNE 8, 2000

Mr. BENNETT (for himself and Mr. SCHUMER) introduced the following bill; which was read twice and referred to the Committee on Armed Services

---

A BILL

To require reports on the progress of the Federal Government in implementing Presidential Decision Directive No. 63 (PDD–63).

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. REPORTS ON FEDERAL GOVERNMENT PROGRESS IN IMPLEMENTING PRESIDENTIAL DECISION DIRECTIVE NO. 63 (PDD–63).

(a) FINDINGS.—Congress makes the following findings:

(1) The protection of our Nation's critical infrastructure is of paramount importance to the security of the United States.

(2) The vulnerability of our Nation's critical sectors—such as financial services, transportation, communications, and energy and water supply—has increased dramatically in recent years as our economy and society have become ever more dependent on interconnected computer systems.

(3) Threats to our Nation's critical infrastructure will continue to grow as foreign governments, terrorist groups, and cyber-criminals increasingly focus on information warfare as a method of achieving their aims.

(4) Addressing the computer-based risks to our Nation's critical infrastructure requires extensive coordination and cooperation within and between Federal agencies and the private sector.

(5) Presidential Decision Directive No. 63 (PDD–63) identifies 12 areas critical to the functioning of the United States and requires certain Federal agencies, and encourages private sector industries, to develop and comply with strategies intended to enhance the Nation's ability to protect its critical infrastructure.

(6) PDD–63 requires lead Federal agencies to work with their counterparts in the private sector to

create early warning information sharing systems and other cyber-security strategies.

(7) PDD–63 further requires that key Federal agencies develop their own internal information assurance plans, and that these plans be fully operational not later than May 2003.

(b) REPORT REQUIREMENTS.—(1) Not later than July 1, 2001, the President shall submit to Congress a comprehensive report detailing the specific steps taken by the Federal Government as of the date of the report to develop infrastructure assurance strategies and the timetable of the Federal Government for operationalizing and fully implementing critical information systems defense by May, 2003. The report shall include the following:

(A) A detailed summary of the progress of each Federal agency in developing an internal information assurance plan.

(B) The progress of Federal agencies in establishing partnerships with relevant private sector industries.

(C) The status of cyber-security and information assurance capabilities in the private sector industries at the forefront of critical infrastructure protection.

(2)(A) Not later than 120 days after the date of the enactment of this Act, the Secretary of Defense shall submit to Congress a detailed report on Department of Defense plans and programs to organize a coordinated defense against attacks on critical infrastructure and critical information-based systems in both the Federal Government and the private sector. The report shall be provided in both classified and unclassified formats.

(B) The report shall include the following:

(i) A description of the current role of the Department of Defense in implementing Presidential Decision Directive No. 63 (PDD–63).

(ii) A description of the manner in which the Department is integrating its various capabilities and assets (including the Army Land Information Warfare Activity (LIWA), the Joint Task Force on Computer Network Defense (JTF–CND), and the National Communications System) into an indications and warning architecture.

(iii) A description of Department work with the intelligence community to identify, detect, and counter the threat of information warfare programs by potentially hostile foreign national governments and sub-national groups.

(iv) A definition of the terms ''nationally significant cyber event'' and ''cyber reconstitution''.

(v) A description of the organization of Department to protect its foreign-based infrastructure and networks.

(vi) An identification of the elements of a defense against an information warfare attack, including the integration of the Computer Network Attack Capability of the United States Space Command into the overall cyber-defense of the United States.

○