AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

I

112TH CONGRESS
2D SESSION

# H. R. 6221

To amend the Homeland Security Act of 2002 to require the Secretary of Homeland Security to research, identify, and evaluate cybersecurity risks to critical infrastructure, and for other purposes.

---

IN THE HOUSE OF REPRESENTATIVES

JULY 26, 2012

Ms. CLARKE of New York (for herself and Mr. DANIEL E. LUNGREN of California) introduced the following bill; which was referred to the Committee on Homeland Security

---

# A BILL

To amend the Homeland Security Act of 2002 to require the Secretary of Homeland Security to research, identify, and evaluate cybersecurity risks to critical infrastructure, and for other purposes.

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

**SECTION 1. SHORT TITLE.**

This Act may be cited as the ''Identifying Cybersecurity Risks to Critical Infrastructure Act of 2012''.

**SEC. 2. IDENTIFICATION OF SECTOR-SPECIFIC CYBERSECURITY RISKS.**

(a) IN GENERAL.—Subtitle C of title II of the Homeland Security Act of 2002 (6 U.S.C. 141 et seq.) is amended by adding at the end the following new section:

**"SEC. 226. IDENTIFICATION OF SECTOR-SPECIFIC CYBERSECURITY RISKS.**

''(a) IN GENERAL.—The Secretary shall, on a continuous and sector-by-sector basis, research, identify, and evaluate cybersecurity risks to critical infrastructure. In carrying out this subsection, the Secretary shall coordinate, as appropriate, with the following:

''(1) The heads of sector specific agencies.

''(2) The owners and operators of critical infrastructure.

''(3) Any private sector entity engaged in ensuring the security or resilience of critical infrastructure, as determined appropriate by the Secretary.

''(b) EVALUATION OF RISKS.—The Secretary, in coordination with the individuals and entities referred to in subsection (a), shall evaluate the cybersecurity risks researched and identified under such subsection by taking into account each of the following:

''(1) The actual or assessed threat, including a consideration of adversary capabilities and intent,

preparedness, target attractiveness, and deterrence capabilities.

''(2) The extent and likelihood of death, injury, or serious adverse effects to human health and safety caused by a disruption, destruction, or unauthorized use of critical infrastructure.

''(3) The threat to national security caused by the disruption, destruction, or unauthorized use of critical infrastructure.

''(4) The harm to the economy that would result from the disruption, destruction, or unauthorized use of critical infrastructure.

''(5) Other risk-based security factors that the Secretary determines appropriate to protect public health and safety, critical infrastructure, or national and economic security, in consultation with the following:

''(A) The heads of sector specific agencies.

''(B) Any private sector entity determined appropriate by the Secretary.

''(c) AVAILABILITY OF IDENTIFIED RISKS.—The Secretary shall ensure that information relating to the risks researched, identified, and evaluated under this section for each sector described in subsection (a) is disseminated, to the maximum extent possible, in an unclassified version,

to owners and operators of critical infrastructure within each such sector. If the Secretary determines that such information, in whole or in part should be classified, the Secretary shall share such information, as the Secretary determines appropriate, with such owners and operators if such owners and operators possess the appropriate security clearances.

''(d) PERIODIC REPORTS TO CONGRESS.—The Secretary shall periodically, but not less often than semiannually, report to the appropriate congressional committees on the cybersecurity risks to critical infrastructure researched, identified, and evaluated pursuant to subsection (a).

''(e) CRITICAL INFRASTRUCTURE DEFINED.—In this section, the term 'critical infrastructure' has the meaning given such term under section 1016(e) of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001 (42 U.S.C. 5195c(e); Public Law 107–56).''.

(b) CLERICAL AMENDMENT.—Subsection (b) of section 1 of the Homeland Security Act of 2002 (6 U.S.C. 101) is amended by adding after the item relating to section 225 the following new item:

''Sec. 226. Identification of sector-specific cybersecurity risks.''.

○