

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.

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 “Identifying Cybersecu-
5 rity Risks to Critical Infrastructure Act of 2012”.

1 **SEC. 2. IDENTIFICATION OF SECTOR-SPECIFIC CYBERSECU-**

2 **RITY RISKS.**

3 (a) IN GENERAL.—Subtitle C of title II of the Home-
4 land Security Act of 2002 (6 U.S.C. 141 et seq.) is amend-
5 ed by adding at the end the following new section:

6 **“SEC. 226. IDENTIFICATION OF SECTOR-SPECIFIC CYBER-**

7 **SECURITY RISKS.**

8 “(a) IN GENERAL.—The Secretary shall, on a contin-
9 uous and sector-by-sector basis, research, identify, and
10 evaluate cybersecurity risks to critical infrastructure. In
11 carrying out this subsection, the Secretary shall coordi-
12 nate, as appropriate, with the following:

13 “(1) The heads of sector specific agencies.

14 “(2) The owners and operators of critical infra-
15 structure.

16 “(3) Any private sector entity engaged in ensur-
17 ing the security or resilience of critical infrastruc-
18 ture, as determined appropriate by the Secretary.

19 “(b) EVALUATION OF RISKS.—The Secretary, in co-
20 ordination with the individuals and entities referred to in
21 subsection (a), shall evaluate the cybersecurity risks re-
22 searched and identified under such subsection by taking
23 into account each of the following:

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

1 preparedness, target attractiveness, and deterrence
2 capabilities.

3 “(2) The extent and likelihood of death, injury,
4 or serious adverse effects to human health and safe-
5 ty caused by a disruption, destruction, or unauthor-
6 ized use of critical infrastructure.

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

10 “(4) The harm to the economy that would re-
11 sult from the disruption, destruction, or unauthor-
12 ized use of critical infrastructure.

13 “(5) Other risk-based security factors that the
14 Secretary determines appropriate to protect public
15 health and safety, critical infrastructure, or national
16 and economic security, in consultation with the fol-
17 lowing:

18 “(A) The heads of sector specific agencies.

19 “(B) Any private sector entity determined
20 appropriate by the Secretary.

21 “(c) AVAILABILITY OF IDENTIFIED RISKS.—The Sec-
22 retary shall ensure that information relating to the risks
23 researched, identified, and evaluated under this section for
24 each sector described in subsection (a) is disseminated, to
25 the maximum extent possible, in an unclassified version,

1 to owners and operators of critical infrastructure within
2 each such sector. If the Secretary determines that such
3 information, in whole or in part should be classified, the
4 Secretary shall share such information, as the Secretary
5 determines appropriate, with such owners and operators
6 if such owners and operators possess the appropriate secu-
7 rity clearances.

8 “(d) PERIODIC REPORTS TO CONGRESS.—The Sec-
9 retary shall periodically, but not less often than semiannu-
10 ally, report to the appropriate congressional committees
11 on the cybersecurity risks to critical infrastructure re-
12 searched, identified, and evaluated pursuant to subsection
13 (a).

14 “(e) CRITICAL INFRASTRUCTURE DEFINED.—In this
15 section, the term ‘critical infrastructure’ has the meaning
16 given such term under section 1016(e) of the Uniting and
17 Strengthening America by Providing Appropriate Tools
18 Required to Intercept and Obstruct Terrorism (USA PA-
19 RIOT ACT) Act of 2001 (42 U.S.C. 5195c(e); Public
20 Law 107–56).”.

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

“Sec. 226. Identification of sector-specific cybersecurity risks.”.

