

7. AN AMENDMENT TO BE OFFERED BY REPRESENTATIVE
ARCURI, MICHAEL OF NEW YORK OR HIS DESIGNEE,
DEBATABLE FOR 10 MINUTES

**AMENDMENT TO H.R. 2701, AS REPORTED
OFFERED BY MR. ARCURI**

Insert after section 354 the following new section:

1 **SEC. 355. CYBERSECURITY OVERSIGHT.**

2 (a) NOTIFICATION OF CYBERSECURITY PRO-
3 GRAMS.—

4 (1) REQUIREMENT FOR NOTIFICATION.—

5 (A) EXISTING PROGRAMS.—Not later than
6 30 days after the date of the enactment of this
7 Act, the President shall submit to Congress a
8 notification for each cybersecurity program in
9 operation on such date that includes the docu-
10 mentation referred to in subparagraphs (A)
11 through (E) of paragraph (2).

12 (B) NEW PROGRAMS.—Not later than 30
13 days after the date of the commencement of op-
14 erations of a new cybersecurity program, the
15 President shall submit to Congress a notifica-
16 tion of such commencement that includes the
17 documentation referred to in subparagraphs (A)
18 through (E) of paragraph (2).

1 (2) DOCUMENTATION.—A notification required
2 by paragraph (1) for a cybersecurity program shall
3 include—

4 (A) the legal justification for the cyberse-
5 curity program;

6 (B) the certification, if any, made pursu-
7 ant to section 2511(2)(a)(ii)(B) of title 18,
8 United States Code, or other statutory certifi-
9 cation of legality for the cybersecurity program;

10 (C) the concept for the operation of the cy-
11 bersecurity program that is approved by the
12 head of the appropriate agency or department;

13 (D) the assessment, if any, of the privacy
14 impact of the cybersecurity program prepared
15 by the privacy or civil liberties protection officer
16 or comparable officer of such agency or depart-
17 ment; and

18 (E) the plan, if any, for independent audit
19 or review of the cybersecurity program to be
20 carried out by the head of the relevant depart-
21 ment or agency of the United States, in con-
22 junction with the appropriate inspector general.

23 (b) PROGRAM REPORTS.—

24 (1) REQUIREMENT FOR REPORTS.—The head of
25 a department or agency of the United States with

1 responsibility for a cybersecurity program for which
2 a notification was submitted under subsection (a), in
3 consultation with the inspector general for that de-
4 partment or agency, shall submit to Congress and
5 the President, in accordance with the schedule set
6 out in paragraph (2), a report on such cybersecurity
7 program that includes—

8 (A) the results of any audit or review of
9 the cybersecurity program carried out under the
10 plan referred to in subsection (a)(2)(E), if any;
11 and

12 (B) an assessment of whether the imple-
13 mentation of the cybersecurity program—

14 (i) is in compliance with—

15 (I) the legal justification referred
16 to in subsection (a)(2)(A); and

17 (II) the assessment referred to in
18 subsection (a)(2)(D), if any;

19 (ii) is adequately described by the con-
20 cept of operation referred to in subsection
21 (a)(2)(C), if any; and

22 (iii) includes an adequate independent
23 audit or review system and whether im-
24 provements to such independent audit or
25 review system are necessary.

1 (2) SCHEDULE FOR SUBMISSION OF RE-
2 REPORTS.—The reports required by paragraph (1)
3 shall be submitted to Congress and the President ac-
4 cording to the following schedule:

5 (A) An initial report shall be submitted not
6 later than 180 days after the date of the enact-
7 ment of this Act.

8 (B) A second report shall be submitted not
9 later than one year after the date of the enact-
10 ment of this Act.

11 (C) Additional reports shall be submitted
12 periodically following the submission of the re-
13 ports referred to in subparagraphs (A) and (B)
14 as necessary, as determined by the head of the
15 relevant department or agency of the United
16 States in conjunction with the inspector general
17 of that department or agency.

18 (3) COOPERATION AND COORDINATION.—

19 (A) COOPERATION.—The head of each de-
20 partment or agency of the United States re-
21 quired to submit a report under paragraph (1)
22 for a particular cybersecurity program, and the
23 inspector general of each such department or
24 agency, shall, to the extent practicable, work in
25 conjunction with any other such head or inspec-

1 tor general required to submit such a report for
2 such cybersecurity program.

3 (B) COORDINATION.—The heads of all of
4 the departments and agencies of the United
5 States required to submit a report under para-
6 graph (1) for a particular cybersecurity pro-
7 gram shall designate one such head to coordi-
8 nate the conduct of the reports on such pro-
9 gram.

10 (c) INFORMATION SHARING REPORT.—Not later
11 than one year after the date of the enactment of this Act,
12 the Inspector General of the Department of Homeland Se-
13 curity and the Inspector General of the Intelligence Com-
14 munity shall jointly submit to Congress and the President
15 a report on the status of the sharing of cyber threat infor-
16 mation, including—

17 (1) a description of how cyber threat intel-
18 ligence information, including classified information,
19 is shared among the agencies and departments of
20 the United States and with persons responsible for
21 critical infrastructure;

22 (2) a description of the mechanisms by which
23 classified cyber threat information is distributed;

24 (3) an assessment of the effectiveness of such
25 information sharing and distribution; and

1 (4) any other matters identified by the Inspec-
2 tors General that would help to fully inform Con-
3 gress or the President regarding the effectiveness
4 and legality of cybersecurity programs.

5 (d) PERSONNEL DETAILS.—

6 (1) AUTHORITY TO DETAIL.—Notwithstanding
7 any other provision of law, the head of an element
8 of the intelligence community that is funded through
9 the National Intelligence Program may detail an of-
10 ficer or employee of such element to the National
11 Cyber Investigative Joint Task Force or to the De-
12 partment of Homeland Security to assist the Task
13 Force or the Department with cybersecurity, as
14 jointly agreed by the head of such element and the
15 Task Force or the Department.

16 (2) BASIS FOR DETAIL.—A personnel detail
17 made under paragraph (1) may be made—

18 (A) for a period of not more than three
19 years; and

20 (B) on a reimbursable or nonreimbursable
21 basis.

22 (e) SUNSET.—The requirements and authorities of
23 this section shall terminate on December 31, 2012.

24 (f) DEFINITIONS.—In this section:

1 (1) CYBERSECURITY PROGRAM.—The term “cy-
2 bersecurity program” means a class or collection of
3 similar cybersecurity operations of an agency or de-
4 partment of the United States that involves person-
5 ally identifiable data that is—

6 (A) screened by a cybersecurity system
7 outside of the agency or department of the
8 United States that was the intended recipient of
9 the personally identifiable data;

10 (B) transferred, for the purpose of cyberse-
11 curity, outside the agency or department of the
12 United States that was the intended recipient of
13 the personally identifiable data; or

14 (C) transferred, for the purpose of cyberse-
15 curity, to an element of the intelligence commu-
16 nity.

17 (2) NATIONAL CYBER INVESTIGATIVE JOINT
18 TASK FORCE.—The term “National Cyber Investiga-
19 tive Joint Task Force” means the multi-agency
20 cyber investigation coordination organization over-
21 seen by the Director of the Federal Bureau of Inves-
22 tigation known as the Nation Cyber Investigative
23 Joint Task Force that coordinates, integrates, and
24 provides pertinent information related to cybersecu-
25 rity investigations.

1 (3) CRITICAL INFRASTRUCTURE.—The term
2 “critical infrastructure” has the meaning given that
3 term in section 1016 of the USA PATRIOT Act (42
4 U.S.C. 5195c).

