

115TH CONGRESS
1ST SESSION

S. 1544

To prevent Federal funds from being used to establish a cybersecurity unit
in cooperation with the Russian Federation.

IN THE SENATE OF THE UNITED STATES

JULY 12, 2017

Ms. KLOBUCHAR (for herself, Mr. CARDIN, Mr. DURBIN, Mr. REED, Ms. WARREN, Mr. SANDERS, Mr. MARKEY, Ms. DUCKWORTH, Mr. FRANKEN, Mr. BLUMENTHAL, Mr. WHITEHOUSE, Mrs. MURRAY, Mrs. SHAHEEN, Ms. HARRIS, and Mr. MERKLEY) introduced the following bill; which was read twice and referred to the Committee on Foreign Relations

A BILL

To prevent Federal funds from being used to establish a
cybersecurity unit in cooperation with the Russian Fed-
eration.

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; TABLE OF CONTENTS.**

4 (a) SHORT TITLE.—This Act may be cited as the
5 “No Funds for Cyber Coordination with Russia Act of
6 2017”.

7 (b) TABLE OF CONTENTS.—The table of contents for
8 this Act is as follows:

Sec. 1. Short title; table of contents.
 Sec. 2. Definitions.
 Sec. 3. Purpose.
 Sec. 4. Findings.
 Sec. 5. Funding prohibition.
 Sec. 6. Sense of Congress.
 Sec. 7. Termination.

1 **SEC. 2. DEFINITIONS.**

2 In this Act:

3 (1) APPROPRIATE CONGRESSIONAL COMMIT-
 4 TEES.—The term “appropriate congressional com-
 5 mittees” means—

6 (A) the Committee on Rules and Adminis-
 7 tration, the Committee on Foreign Relations,
 8 the Committee on Armed Services, the Com-
 9 mittee on Homeland Security and Govern-
 10 mental Affairs, the Committee on Appropria-
 11 tions, and the Select Committee on Intelligence
 12 of the Senate; and

13 (B) the Committee on Foreign Affairs, the
 14 Committee on House Administration, the Com-
 15 mittee on Armed Services, the Committee on
 16 Homeland Security, the Committee on Appro-
 17 priations, and the Permanent Select Committee
 18 on Intelligence of the House of Representatives.

19 (2) CYBERSECURITY.—The term “cybersecu-
 20 rity” means the protection or defense of cyberspace
 21 from cyberattacks.

1 (3) CYBERSECURITY UNIT.—The term “cyber-
2 security unit” means any organization or entity es-
3 tablished for the purpose of cybersecurity.

4 (4) CYBERSPACE.—The term “cyberspace”
5 means the global domain within the information en-
6 vironment consisting of the interdependent network
7 of information systems infrastructures (including the
8 Internet, telecommunications networks, computer
9 systems, and embedded processors and controllers).

10 (5) SIGNIFICANT ACTIVITIES UNDERMINING CY-
11 BERSECURITY.—The term “significant activities un-
12 dermining cybersecurity” includes—

13 (A) significant efforts—

14 (i) to deny access to or degrade, dis-
15 rupt, or destroy an information and com-
16 munications technology system or network;
17 or

18 (ii) to exfiltrate, degrade, corrupt, de-
19 stroy, or release information from such a
20 system or network without authorization
21 for purposes of—

22 (I) conducting influence oper-
23 ations; or

24 (II) causing a significant mis-
25 appropriation of funds, economic re-

1 sources, trade secrets, personal identi-
2 fications, or financial information for
3 commercial or competitive advantage
4 or private financial gain;

5 (B) significant destructive malware at-
6 tacks; and

7 (C) significant denial of service activities.

8 **SEC. 3. PURPOSE.**

9 The purpose of this Act is to protect United States
10 cybersecurity and critical infrastructure by preventing the
11 President from establishing a cybersecurity unit in coordi-
12 nation with the Government of the Russian Federation,
13 a known foreign adversary.

14 **SEC. 4. FINDINGS.**

15 Congress makes the following findings:

16 (1) On January 6, 2017, an assessment of the
17 United States intelligence community entitled, “As-
18 sessing Russian Activities and Intentions in Recent
19 U.S. Elections” concluded, “Russian efforts to influ-
20 ence the 2016 U.S. presidential election represent
21 the most recent expression of Moscow’s longstanding
22 desire to undermine the U.S.-led liberal democratic
23 order, but these activities demonstrated a significant
24 escalation in directness, level of activity, and scope
25 of effort compared to previous operations.” The re-

1 port concluded with high confidence, “Russian Presi-
2 dent Vladimir Putin ordered an influence campaign
3 in 2016 aimed at the U.S. presidential election. Rus-
4 sia’s goals were to undermine public faith in the
5 U.S. democratic process, denigrate Secretary Clin-
6 ton, and harm her electability and potential presi-
7 dency. We further assess Putin and the Russian
8 Government developed a clear preference for Presi-
9 dent-elect Trump.”.

10 (2) On December 29, 2016, President Barack
11 Obama issued Executive Order 13757, “Taking Ad-
12 ditional Steps To Address The National Emergency
13 With Respect To Significant Malicious Cyber-En-
14 abled Activities”. Executive Order 13757 amended
15 Executive Order 13694, “Blocking the Property of
16 Certain Persons Engaging in Significant Malicious
17 Cyber-Enabled Activities”. E.O. 13694 authorized
18 sanctions on “individuals and entities determined to
19 be responsible for or complicit in malicious cyber-en-
20 abled activities that result in enumerated harms that
21 are reasonably likely to result in, or have materially
22 contributed to, a significant threat to the national
23 security, foreign policy, or economic health or finan-
24 cial stability of the United States”. E.O. 13757 ex-
25 panded executive authority to allow for the imposi-

1 tion of sanctions against “individuals and entities
2 determined to be responsible for tampering, altering,
3 or causing the misappropriation of information with
4 the purpose or effect of interfering with or under-
5 mining election processes or institutions”.

6 (3) The Government of the Russian Federation
7 has repeatedly launched cyber-attacks against
8 United States agencies, including the Department of
9 State in November 2014, the Department of De-
10 fense in 2015, and the White House computer net-
11 works in 2014.

12 (4) On March 15, 2017, the Department of
13 Justice charged Russian Federal Security Service
14 (FSB) officers and criminal coconspirators for hack-
15 ing Yahoo and the email accounts of millions of
16 United States citizens.

17 (5) On May 8, 2017, former Director of Na-
18 tional Intelligence James Clapper testified before the
19 Committee on the Judiciary of the Senate, “Russia’s
20 influence activities in the run-up to the 2016 elec-
21 tion constituted the high water mark of their long
22 running efforts since the 1960s to disrupt and influ-
23 ence our elections. They must be congratulating
24 themselves for having exceeded their wildest expecta-
25 tions with a minimal expenditure of resource. And I

1 believe they are now emboldened to continue such
2 activities in the future both here and around the
3 world, and to do so even more intensely. If there has
4 ever been a clarion call for vigilance and action
5 against a threat to the very foundation of our demo-
6 cratic political system, this episode is it.”.

7 (6) On June 7, 2017, former Director of the
8 Federal Bureau of Investigations James Comey tes-
9 tified before the Select Committee on Intelligence of
10 the Senate that the Government of the Russian Fed-
11 eration, “using technical intrusion, lots of other
12 methods, tried to shape the way we think, we vote,
13 we act. That is a big deal. And people need to recog-
14 nize it. It’s not about Republicans or Democrats.
15 They’re coming after America, which I hope we all
16 love equally. They want to undermine our credibility
17 in the face of the world. They think that this great
18 experiment of ours is a threat to them, and so
19 they’re going to try to run it down and dirty it up
20 as much as possible.”.

21 (7) On July 9, 2017, President Donald Trump
22 stated, “I strongly pressed President Putin twice
23 about Russian meddling in our election. He vehe-
24 mently denied it . . . now it is time to move forward
25 in working constructively with Russia! Putin & I dis-

1 cussed forming an impenetrable Cyber Security unit
2 so that election hacking, & many other negative
3 things, will be guarded”.

4 **SEC. 5. FUNDING PROHIBITION.**

5 No Federal funds may be used to establish a cyberse-
6 curity unit, or any variation thereof, in cooperation or con-
7 nection with the Government of the Russian Federation.

8 **SEC. 6. SENSE OF CONGRESS.**

9 It is the sense of Congress that—

10 (1) the President should publicly endorse the
11 assessment of the United States Armed Forces and
12 the intelligence community that the Government of
13 the Russian Federation interfered in the 2016 elec-
14 tion and take appropriate measures to deter such ac-
15 tivities in the future;

16 (2) the President must not use taxpayer funds
17 to engage in cyber coordination with the Government
18 of the Russian Federation, a foreign adversary; and

19 (3) the President should work with Congress to
20 establish a non-partisan, independent commission of
21 experts to determine, examine, and report on the
22 facts regarding the extent of Russian official and
23 unofficial cyber operations and other attempts to
24 interfere in the 2016 United States national election.

1 **SEC. 7. TERMINATION.**

2 The prohibitions under this Act shall terminate on
3 the date the President submits to the appropriate congres-
4 sional committees a written certification that the Govern-
5 ment of the Russian Federation has—

6 (1) ceased ordering, controlling, or otherwise di-
7 recting, supporting, or financing acts intended to
8 undermine democracies around the world; and

9 (2) submitted a written statement acknowl-
10 edging interference in the 2016 United States Presi-
11 dential election.

○