

114TH CONGRESS
2D SESSION

S. _____

To require all Department of State employees to use Department-managed email accounts and telephonic systems for all work-related electronic communications, to require the Secretary of State to submit an annual report to Congress on any security violations within the Department, to provide training to Department of State employees on the rules and procedures governing the appropriate handling of classified information, to reform the process for identifying and archiving classified information, and for other purposes.

IN THE SENATE OF THE UNITED STATES

Mr. PERDUE (for himself, Mr. SASSE, and Mr. ISAKSON) introduced the following bill; which was read twice and referred to the Committee on

A BILL

To require all Department of State employees to use Department-managed email accounts and telephonic systems for all work-related electronic communications, to require the Secretary of State to submit an annual report to Congress on any security violations within the Department, to provide training to Department of State employees on the rules and procedures governing the appropriate handling of classified information, to reform the process for identifying and archiving classified information, 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 “Securing our Secrets
5 Act” or the “SOS Act”.

6 **SEC. 2. DEFINITIONS.**

7 In this Act:

8 (1) APPROPRIATE CONGRESSIONAL COMMIT-
9 TEES.—The term “appropriate congressional com-
10 mittees” means—

11 (A) the Committee on Foreign Relations of
12 the Senate;

13 (B) the Select Committee on Intelligence
14 of the Senate;

15 (C) the Committee on Foreign Affairs of
16 the House of Representatives; and

17 (D) the Permanent Select Committee on
18 Intelligence of the House of Representatives.

19 (2) DEPARTMENT.—The term “Department”
20 means the Department of State.

21 (3) INFRACTION; VIOLATION.—The terms “in-
22 fraction” and “violation” have the meanings given
23 such terms in section 6.1 of Executive Order 13526
24 (2009).

1 (4) INSPECTOR GENERAL.—The term “Inspec-
2 tor General” means the Inspector General for the
3 Department of State and the Broadcasting Board of
4 Governors.

5 (5) INTELLIGENCE COMMUNITY.—The term
6 “intelligence community” has the meaning given
7 that term in section 3(4) of the National Security
8 Act of 1947 (50 U.S.C. 3003(4)).

9 (6) SECRETARY.—The term “Secretary” means
10 the Secretary of State.

11 **SEC. 3. USE OF NONGOVERNMENTAL INFORMATION SYS-**
12 **TEMS.**

13 (a) IN GENERAL.—Beginning not later than 30 days
14 after the date of the enactment of this Act, employees of
15 the Department may only use, for all electronic commu-
16 nications related to their work for the Department—

17 (1) email accounts on state.gov that are owned
18 and managed by the Department;

19 (2) telephonic systems that are owned and man-
20 aged by the Department; or

21 (3) other electronic communications systems
22 owned and managed by the Department or another
23 appropriate Federal agency, whenever such systems
24 are available.

25 (b) CERTIFICATION AND REPORTING.—

1 (1) CERTIFICATION.—Except as provided in
2 paragraphs (2) and (3), not later than 90 days after
3 the date of the enactment of this Act, and annually
4 thereafter, the Secretary shall certify in writing to
5 the appropriate congressional committees that all
6 employees of the Department have been provided
7 with access to electronic communications systems de-
8 scribed in subsection (a).

9 (2) REPORTING.—If the Secretary cannot make
10 the certification described in paragraph (1), the Sec-
11 retary shall submit a report to the appropriate con-
12 gressional committees that identifies—

13 (A) the number of employees of the De-
14 partment who lack access to electronic commu-
15 nications systems described in subsection (a);

16 (B) the reasons for such lack of access;

17 (C) the steps that have been taken to en-
18 sure that such employees obtain and maintain
19 such access on a reliable basis; and

20 (D) the steps that have been taken to en-
21 sure that work-related electronic communica-
22 tions by such employees are appropriately re-
23 corded, archived, and reviewed for the potential
24 presence of classified information.

1 (3) WAIVER.—On a case by case basis, the Sec-
2 retary of State may waive the requirements under
3 subsection (a) for one employee, or a group of up to
4 10 employees, if, not later than 7 days after grant-
5 ing such waiver, the Secretary—

6 (A) certifies in writing to the appropriate
7 congressional committees that—

8 (i) such waiver is in the foreign policy
9 or national security interest of the United
10 States; and

11 (ii) all work-related written commu-
12 nications generated by or processed on
13 nongovernmental systems by employees
14 subject to such waiver will be appropriately
15 archived in accordance with chapters 21,
16 29, 31, and 33 of title 44, United States
17 Code (commonly referred to as the “Fed-
18 eral Records Act”) and all related rules,
19 regulations, guidance, and Executive Or-
20 ders; and

21 (B) provides a written justification for
22 such waiver to the appropriate congressional
23 committees.

24 (4) LIMITATIONS.—

1 (A) DURATION.—Waivers issued pursuant
2 to paragraph (3) shall be valid for up to 180
3 days, but may be reissued by the Secretary in
4 accordance with the requirements under para-
5 graph (3).

6 (B) MULTIPLE WAIVERS.—The Secretary
7 may issue multiple waivers under paragraph (3)
8 if each waiver is consistent with the certifi-
9 cation and the accompanying justification.

10 (5) ACCOUNTABILITY.—Not later than 90 days
11 after the date of the enactment of this Act, the In-
12 spector General shall develop and implement an
13 oversight plan designed to determine, to the greatest
14 extent practicable, whether the Secretary and all
15 other employees of the Department are in full com-
16 pliance with the requirements under this section.

17 **SEC. 4. REPORT ON SECURITY REVIEWS AND VIOLATIONS.**

18 (a) IN GENERAL.—Not later than 90 days after the
19 date of the enactment of this Act, and annually thereafter,
20 the Secretary shall submit a report to the appropriate con-
21 gressional committees that details every security violation,
22 including the unauthorized transfer of marked or un-
23 marked classified information into documents, electronic
24 media or systems, electronic transmissions, or other
25 records or storage not certified for the handling, storage,

1 or transmittal of such information, that occurred during
2 the most recently completed fiscal year.

3 (b) CONTENTS.—The report required under sub-
4 section (a) shall include, for each security violation identi-
5 fied in the report—

6 (1) the name and title of the employee respon-
7 sible for the violation;

8 (2) the date of the violation;

9 (3) a description of the violation, including
10 whether or not there is any indication that classified
11 information was compromised;

12 (4) the statute, rule, Executive order, or regula-
13 tion that was violated; and

14 (5) a description of actions taken by officials of
15 the Department in response to the violation, includ-
16 ing—

17 (A) any disciplinary action taken or crimi-
18 nal referral made against the employee involved;
19 and

20 (B) any remedial training administered to
21 the employee involved or to other employees of
22 the Department; and

23 (6) if the employee responsible for the violation
24 had committed one or more additional security viola-
25 tions during the prior 10 years and the Secretary

1 did not terminate the employee or request the Fed-
2 eral Bureau of Investigations to review the violation,
3 a justification for failing to take such actions.

4 (c) PRIVACY ACT PROTECTIONS.—The report re-
5 quired under subsection (a)—

6 (1) may not be made public by the Department;
7 and

8 (2) shall be transmitted in such a manner so as
9 to prevent the public dissemination of any informa-
10 tion protected under the Privacy Act of 1974 (5
11 U.S.C. 552a et seq.).

12 **SEC. 5. CLASSIFIED INFORMATION SPILLAGE.**

13 (a) DETECTION OF CLASSIFIED INFORMATION
14 SPILLAGE.—The Secretary shall appoint appropriate offi-
15 cials of the Bureau of Diplomatic Security to receive train-
16 ing, in coordination with the Office of the Director of Na-
17 tional Intelligence, in the recognition of classified informa-
18 tion spillage.

19 (b) RANDOMIZED SAMPLING TO DETECT SPILL-
20 AGE.—Each quarter, the officials appointed pursuant to
21 subsection (a) shall—

22 (1) collect statistically valid random samples of
23 emails sent by or received from employees of the De-
24 partment who hold a security clearance granting

1 them authorized access to information classified at
2 the level of Secret or above; and

3 (2) use such randomized sampling, in accord-
4 ance with the training received under subsection (a),
5 to detect classified information spillage as part of
6 the Department's program for safeguarding classi-
7 fied information.

8 (c) ACCOUNTABILITY.—The Inspector General
9 shall—

10 (1) audit the work described in subsection (b);
11 and

12 (2) include the findings of such audits in the
13 semiannual reports submitted to the appropriate
14 congressional committees.

15 **SEC. 6. REMEDIAL TRAINING.**

16 (a) EMERGENCY REFRESHER TRAINING.—Not later
17 than 180 days after the date of the enactment of this Act,
18 the Secretary shall certify in writing to the appropriate
19 congressional committees that all personnel of the Depart-
20 ment who possess security clearances have completed the
21 emergency refresher training described in subsection (b).

22 (b) CONTENTS.—The Secretary shall require all per-
23 sonnel of the Department who possess security clearances
24 to complete emergency refresher training on the rules and

1 procedures governing the appropriate handling of classi-
2 fied information, including—

3 (1) applicable rules and procedures governing—

4 (A) the receipt, handling, and transmission
5 of classified information by electronic means,
6 including telephonic, text message, facsimile,
7 and email communications;

8 (B) derivative classification, and the imper-
9 ative of continuing to safeguard classified infor-
10 mation when drawing upon such information in
11 the creation of secondary documents or other
12 communications;

13 (C) the receipt, handling, and transmission
14 of foreign government information (as defined
15 in section 6.1(s) of Executive Order 13526
16 (2009)), and the requirements set forth in sec-
17 tions 1.1(d) and 4.1(h) of such Executive order;

18 (D) the review and processing of requests
19 for information under section 552 of title 5,
20 United States Code (commonly known as the
21 “Freedom of Information Act”);

22 (E) challenges to classification status, in-
23 cluding section 1.8 of Executive Order 13526
24 (2009); and

1 (F) the continued protection of classified
2 information that has been disclosed without au-
3 thorization, including the requirement under
4 section 1.1(c) of Executive Order 13526 (2009)
5 that “[c]lassified information shall not be de-
6 classified automatically as a result of any unau-
7 thorized disclosure of identical or similar infor-
8 mation”;

9 (2) the requirement under section 5.4 of Execu-
10 tive Order 13526 (2009) that the Secretary—

11 (A) “demonstrate personal commitment
12 and commit senior management to the success-
13 ful implementation of the program established
14 under this order”;

15 (B) “commit necessary resources to the ef-
16 fective implementation” of programs for the
17 handling and protection of classified informa-
18 tion;

19 (C) “ensure that agency records systems
20 are designed and maintained to optimize the
21 appropriate sharing and safeguarding of classi-
22 fied information”;

23 (D) “designate a senior agency official to
24 direct and administer the program,”; and

1 (E) include “the designation and manage-
2 ment of classified information” as a critical ele-
3 ment or item to be evaluated in personnel per-
4 formance evaluations;

5 (3) a list and clear explanation of the penalties
6 provided for violations of applicable rules and proce-
7 dures governing the topics described in paragraphs
8 (1) and (2); and

9 (4) a signed certification by the employee re-
10 ceiving such retraining that he or she—

11 (A) has received such training;

12 (B) has read and understands the rules,
13 procedures, and penalties described in para-
14 graphs (1) through (3);

15 (C) understands the grave responsibilities
16 entailed by the privilege of being given access to
17 national security information; and

18 (D) undertakes under penalty of all appli-
19 cable laws, regulations, and policies not to vio-
20 late any of such rules and procedures.

21 (c) PRIORITIZATION.—The Secretary shall prioritize
22 the emergency refresher training described in subsection
23 (b) in the following order:

1 (1) Employees possessing security clearances at
2 the Top Secret/Sensitive Compartmented Informa-
3 tion level.

4 (2) Employees cleared for Top Secret informa-
5 tion and below.

6 (3) Employees cleared for Secret information
7 and below.

8 (4) Employees only cleared for Confidential in-
9 formation.

10 (d) WAIVER.—The Secretary may delay the adminis-
11 tration of the emergency refresher training described in
12 subsection (b) for any specific employee or group of em-
13 ployees, up to the level of an individual office, for a period
14 of up to 30 days if the Secretary—

15 (1) determines that the critical foreign policy
16 interests of the United States require such a delay;
17 and

18 (2) provides the appropriate congressional com-
19 mittees with written notice of such delay and an ex-
20 planation of the need for such delay.

21 (e) APPLICABLE RULES AND PROCEDURES DE-
22 FINED.—In this section, the term “applicable rules and
23 procedures” means—

24 (1) any applicable Federal statute;

1 (2) all the requirements set forth on the topic
2 in question by Executive Order 13526 (2009);

3 (3) any other current Executive order dealing
4 with the handling of classified information;

5 (4) the Foreign Affairs Manual of the Depart-
6 ment; and

7 (5) any other Departmental guidance or regula-
8 tions.

9 **SEC. 7. ENDURING TRAINING PROGRAM TO PREVENT MIS-**
10 **HANDLING OF INTELLIGENCE INFORMATION.**

11 Not later than 180 days after the date of the enact-
12 ment of this Act, the Secretary shall establish an enduring
13 training program, which shall be administered annually to
14 all employees of the Department, on how to prevent the
15 transfer of marked or unmarked classified or sensitive in-
16 formation to documents, messages, electronic media, or
17 any other system not certified for the handling or storage
18 of information with that level of classification or sensitivity
19 and compliant with applicable Federal Information Secu-
20 rity Management Act standards, including during the re-
21 view or public release of any record pursuant to section
22 552 of title 5, United States Code (commonly known as
23 the “Freedom of Information Act”).

1 **SEC. 8. PLAN FOR REFORMING RESPONSE TO REQUESTS**
2 **FOR INFORMATION AND INFORMATION**
3 **ARCHIVING.**

4 (a) REQUIREMENT FOR PLAN.—Not later than 90
5 days after the date of the enactment of this Act, the Sec-
6 retary shall submit a plan to the appropriate congressional
7 committees for completing the reforms described in sub-
8 section (b) not later than one year after the date of the
9 enactment of this Act.

10 (b) ELEMENTS.—The plan required under subsection
11 (a) shall include—

12 (1) a process for developing and implementing,
13 in coordination with the Director of National Intel-
14 ligence, a program for training and maintaining an
15 appropriate number of employees of the Department
16 in—

17 (A) identifying marked or unmarked classi-
18 fied information in documents or media subject
19 to requests under section 552 of title 5, United
20 States Code (commonly known as the “Freedom
21 of Information Act”), including information
22 originating with the intelligence community;
23 and

24 (B) the appropriate procedures for ensur-
25 ing that officials from the intelligence commu-
26 nity have an opportunity to make a classifica-

1 tion determination regarding the classification
2 status and level, if any, of any information po-
3 tentially originating with the intelligence com-
4 munity;

5 (2) a process for developing and implementing
6 a training program for all officials of the Depart-
7 ment on how to archive emails and other electronic
8 communications in accordance with chapters 21, 29,
9 31, and 33 of title 44, United States Code, and all
10 related rules, regulations, guidance, and Executive
11 orders; and

12 (3) a requirement for the annual administration
13 of a sworn affidavit made by each employee of the
14 Department certifying that such employee has, to
15 the best of the employee's knowledge and ability,
16 archived all documents (including emails) created or
17 received by such employee in accordance with the
18 chapters 21, 29, 31, and 33 of title 44, United
19 States Code, and all related rules, regulations, guid-
20 ance, and Executive orders.

21 (c) ACCOUNTABILITY.—Not later than one year after
22 the date of the enactment of this Act, the Inspector Gen-
23 eral, after reviewing the implementation of the plan re-
24 quired under this section, shall report to the appropriate

1 congressional committees on the degree to which the Sec-
2 retary—

3 (1) has implemented such plan; and

4 (2) has made progress in ensuring appropriate
5 archiving and securing of information by the De-
6 partment.