114TH CONGRESS
2D SESSION

S. 3160

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

JULY 12, 2016

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

---

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.

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 ''Securing our Secrets Act'' or the ''SOS Act''.

SEC. 2. DEFINITIONS.

In this Act:

(1) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term ''appropriate congressional committees'' means—

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

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

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

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

(2) DEPARTMENT.—The term ''Department'' means the Department of State.

(3) INFRACTION; VIOLATION.—The terms ''infraction'' and ''violation'' have the meanings given such terms in section 6.1 of Executive Order 13526 (2009).

(4) INSPECTOR GENERAL.—The term ''Inspector General'' means the Inspector General for the Department of State and the Broadcasting Board of Governors.

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

(6) SECRETARY.—The term ''Secretary'' means the Secretary of State.

SEC. 3. USE OF NONGOVERNMENTAL INFORMATION SYSTEMS.

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

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

(2) telephonic systems that are owned and managed by the Department; or

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

(b) CERTIFICATION AND REPORTING.—

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

(2) REPORTING.—If the Secretary cannot make the certification described in paragraph (1), the Secretary shall submit a report to the appropriate congressional committees that identifies—

(A) the number of employees of the Department who lack access to electronic communications systems described in subsection (a);

(B) the reasons for such lack of access;

(C) the steps that have been taken to ensure that such employees obtain and maintain such access on a reliable basis; and

(D) the steps that have been taken to ensure that work-related electronic communications by such employees are appropriately recorded, archived, and reviewed for the potential presence of classified information.

(3) WAIVER.—On a case by case basis, the Secretary of State may waive the requirements under subsection (a) for one employee, or a group of up to 10 employees, if, not later than 7 days after granting such waiver, the Secretary—

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

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

(ii) all work-related written communications generated by or processed on nongovernmental systems by employees subject to such waiver will be appropriately archived in accordance with chapters 21, 29, 31, and 33 of title 44, United States Code (commonly referred to as the ''Federal Records Act'') and all related rules, regulations, guidance, and executive orders; and

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

(4) LIMITATIONS.—

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

(B) MULTIPLE WAIVERS.—The Secretary may issue multiple waivers under paragraph (3) if each waiver is consistent with the certification and the accompanying justification.

(5) ACCOUNTABILITY.—Not later than 90 days after the date of the enactment of this Act, the Inspector General shall develop and implement an oversight plan designed to determine, to the greatest extent practicable, whether the Secretary and all other employees of the Department are in full compliance with the requirements under this section.

SEC. 4. REPORT ON SECURITY REVIEWS AND VIOLATIONS.

(a) IN GENERAL.—Not later than 90 days after the date of the enactment of this Act, and annually thereafter, the Secretary shall submit a report to the appropriate congressional committees that details every security violation, including the unauthorized transfer of marked or unmarked classified information into documents, electronic media or systems, electronic transmissions, or other records or storage not certified for the handling, storage,

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

(b) CONTENTS.—The report required under subsection (a) shall include, for each security violation identified in the report—

(1) the name and title of the employee responsible for the violation;

(2) the date of the violation;

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

(4) the statute, rule, executive order, or regulation that was violated; and

(5) a description of actions taken by officials of the Department in response to the violation, including—

(A) any disciplinary action taken or criminal referral made against the employee involved; and

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

(6) if the employee responsible for the violation had committed one or more additional security violations during the prior 10 years and the Secretary

did not terminate the employee or request the Federal Bureau of Investigations to review the violation, a justification for failing to take such actions.

(c) PRIVACY ACT PROTECTIONS.—The report required under subsection (a)—

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

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

SEC. 5. CLASSIFIED INFORMATION SPILLAGE.

(a) DETECTION OF CLASSIFIED INFORMATION SPILLAGE.—The Secretary shall appoint appropriate officials of the Bureau of Diplomatic Security to receive training, in coordination with the Office of the Director of National Intelligence, in the recognition of classified information spillage.

(b) RANDOMIZED SAMPLING TO DETECT SPILLAGE.—Each quarter, the officials appointed pursuant to subsection (a) shall—

(1) collect statistically valid random samples of emails sent by or received from employees of the Department who hold a security clearance granting

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

(2) use such randomized sampling, in accordance with the training received under subsection (a), to detect classified information spillage as part of the Department's program for safeguarding classified information.

(c) ACCOUNTABILITY.—The Inspector General shall—

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

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

SEC. 6. REMEDIAL TRAINING.

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

(b) CONTENTS.—The Secretary shall require all personnel of the Department who possess security clearances to complete emergency refresher training on the rules and

procedures governing the appropriate handling of classified information, including—

(1) applicable rules and procedures governing—

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

(B) derivative classification, and the imperative of continuing to safeguard classified information when drawing upon such information in the creation of secondary documents or other communications;

(C) the receipt, handling, and transmission of foreign government information (as defined in section 6.1(s) of Executive Order 13526 (2009)), and the requirements set forth in sections 1.1(d) and 4.1(h) of such executive order;

(D) the review and processing of requests for information under section 552 of title 5, United States Code (commonly known as the ''Freedom of Information Act'');

(E) challenges to classification status, including section 1.8 of Executive Order 13526 (2009); and

(F) the continued protection of classified information that has been disclosed without authorization, including the requirement under section 1.1(c) of Executive Order 13526 (2009) that ''[c]lassified information shall not be declassified automatically as a result of any unauthorized disclosure of identical or similar information'';

(2) the requirement under section 5.4 of Executive Order 13526 (2009) that the Secretary—

(A) ''demonstrate personal commitment and commit senior management to the successful implementation of the program established under this order'';

(B) ''commit necessary resources to the effective implementation'' of programs for the handling and protection of classified information;

(C) ''ensure that agency records systems are designed and maintained to optimize the appropriate sharing and safeguarding of classified information'';

(D) ''designate a senior agency official to direct and administer the program,''; and

(E) include ''the designation and management of classified information'' as a critical element or item to be evaluated in personnel performance evaluations;

(3) a list and clear explanation of the penalties provided for violations of applicable rules and procedures governing the topics described in paragraphs (1) and (2); and

(4) a signed certification by the employee receiving such retraining that he or she—

(A) has received such training;

(B) has read and understands the rules, procedures, and penalties described in paragraphs (1) through (3);

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

(D) undertakes under penalty of all applicable laws, regulations, and policies not to violate any of such rules and procedures.

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

(1) Employees possessing security clearances at the Top Secret/Sensitive Compartmented Information level.

(2) Employees cleared for Top Secret information and below.

(3) Employees cleared for Secret information and below.

(4) Employees only cleared for Confidential information.

(d) WAIVER.—The Secretary may delay the administration of the emergency refresher training described in subsection (b) for any specific employee or group of employees, up to the level of an individual office, for a period of up to 30 days if the Secretary—

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

(2) provides the appropriate congressional committees with written notice of such delay and an explanation of the need for such delay.

(e) APPLICABLE RULES AND PROCEDURES DEFINED.—In this section, the term ''applicable rules and procedures'' means—

(1) any applicable Federal statute;

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

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

(4) the Foreign Affairs Manual of the Department; and

(5) any other Departmental guidance or regulations.

SEC. 7. ENDURING TRAINING PROGRAM TO PREVENT MISHANDLING OF INTELLIGENCE INFORMATION.

Not later than 180 days after the date of the enactment of this Act, the Secretary shall establish an enduring training program, which shall be administered annually to all employees of the Department, on how to prevent the transfer of marked or unmarked classified or sensitive information to documents, messages, electronic media, or any other system not certified for the handling or storage of information with that level of classification or sensitivity and compliant with applicable Federal Information Security Management Act standards, including during the review or public release of any record pursuant to section 552 of title 5, United States Code (commonly known as the ''Freedom of Information Act'').

SEC. 8. PLAN FOR REFORMING RESPONSE TO REQUESTS FOR INFORMATION AND INFORMATION ARCHIVING.

(a) REQUIREMENT FOR PLAN.—Not later than 90 days after the date of the enactment of this Act, the Secretary shall submit a plan to the appropriate congressional committees for completing the reforms described in subsection (b) not later than one year after the date of the enactment of this Act.

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

(1) a process for developing and implementing, in coordination with the Director of National Intelligence, a program for training and maintaining an appropriate number of employees of the Department in—

(A) identifying marked or unmarked classified information in documents or media subject to requests under section 552 of title 5, United States Code (commonly known as the ''Freedom of Information Act''), including information originating with the intelligence community; and

(B) the appropriate procedures for ensuring that officials from the intelligence community have an opportunity to make a classifica-

tion determination regarding the classification status and level, if any, of any information potentially originating with the intelligence community;

(2) a process for developing and implementing a training program for all officials of the Department on how to archive emails and other electronic communications in accordance with chapters 21, 29, 31, and 33 of title 44, United States Code, and all related rules, regulations, guidance, and executive orders; and

(3) a requirement for the annual administration of a sworn affidavit made by each employee of the Department certifying that such employee has, to the best of the employee's knowledge and ability, archived all documents (including emails) created or received by such employee in accordance with the chapters 21, 29, 31, and 33 of title 44, United States Code, and all related rules, regulations, guidance, and executive orders.

(c) ACCOUNTABILITY.—Not later than one year after the date of the enactment of this Act, the Inspector General, after reviewing the implementation of the plan required under this section, shall report to the appropriate

congressional committees on the degree to which the Secretary—

(1) has implemented such plan; and

(2) has made progress in ensuring appropriate archiving and securing of information by the Department.

○