I

117TH CONGRESS
2D SESSION

H. R. 8403

To encourage and improve Federal proactive cybersecurity initiatives, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

JULY 15, 2022

Mr. SWALWELL introduced the following bill; which was referred to the Committee on Oversight and Reform, and in addition to the Committee on Armed Services, for a period to be subsequently determined by the Speaker, in each case for consideration of such provisions as fall within the jurisdiction of the committee concerned

---

A BILL

To encourage and improve Federal proactive cybersecurity initiatives, 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; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the ''Proactive Cyber Initiatives Act of 2022''.

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

SEC. 2. DEFINITIONS.

In this Act:

(1) ACTIVE DEFENSE TECHNIQUE.—The term ''active defense technique'' means an action taken on an information system of an agency to increase the security of such system against an attacker, including—

(A) the use of a deception technology or other purposeful feeding of false or misleading information to an attacker accessing such system; and

(B) proportional action taken in response to an unlawful breach.

(2) AGENCY.—The term ''agency'' means any Government corporation, Government-controlled corporation, or other establishment of the executive branch of the Government (including the Executive Office of the President), or any independent regulatory agency, but does not include the following:

(A) The Government Accountability Office.

(B) The Federal Election Commission.

(C) The governments of the District of Columbia and of the territories and possessions of

the United States, and their various subdivisions.

(D) Government-owned contractor-operated facilities, including laboratories engaged in national defense research and production activities.

(3) CONTINUOUS MONITORING.—The term ''continuous monitoring'' means continuous experimentation conducted by an agency on an information system of such agency to evaluate the resilience of such system against a malicious attack or condition that could compromise such system for the purpose of improving design, resilience, or incident response with respect to such system.

(4) DECEPTION TECHNOLOGY.—The term ''deception technology'' means an isolated digital environment, system, or platform containing a replication of an active information system with realistic data flows used to attract, mislead, or observe an attacker.

(5) DEPARTMENT.—The term ''department'' means the following:

(A) The Department of State.

(B) The Department of the Treasury.

(C) The Department of Defense.

(D) The Department of Justice.

(E) The Department of the Interior.

(F) The Department of Agriculture.

(G) The Department of Commerce.

(H) The Department of Labor.

(I) The Department of Health and Human Services.

(J) The Department of Housing and Urban Development.

(K) The Department of Transportation.

(L) The Department of Energy.

(M) The Department of Education.

(N) The Department of Veterans Affairs.

(O) The Department of Homeland Security.

(6) DIRECTOR.—The term ''Director'' means the Director of the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security.

(7) INFORMATION SYSTEM.—The term ''information system'' has the meaning given the term in section 3502 of title 44, United States Code.

(8) NATIONAL LABORATORY.—The term ''national laboratory'' has the meaning given the term in

section 2 of the Energy Policy Act of 2005 (42 U.S.C. 15801).

(9) PENETRATION TEST; PENETRATION TESTING.—The terms ''penetration test'' and ''penetration testing'' mean an assessment conducted on an information system of an agency that emulates an attack or other exploitation capability to identify and test vulnerabilities that could be exploited.

(10) RULES OF ENGAGEMENT.—The term ''rules of engagement'' means a set of rules established by an agency for use during penetration testing.

SEC. 3. INCREASING PROACTIVE CYBERSECURITY INITIATIVES.

(a) PENETRATION TESTING.—

(1) IN GENERAL.—The head of each department or agency shall carry out the following:

(A) Conduct regular penetration testing on the information systems (as described in paragraph (2)) of such department or agency.

(B) Provide to the Director, the National Cyber Director, and the Director of the Office of Management and Budget a report on the results of such testing, including—

(i) an identification of any risks discovered; and

(ii) a description of how cybersecurity at such department or agency may be improved.

(2) INFORMATION SYSTEMS DESCRIBED.—For purposes of paragraph (1)(A), an information system of an agency to be tested is one described as moderate- or high-impact in the document titled ''Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy'' (National Institute of Standards and Technology Special Publication 800–37, Revision 2; December 2018) or in a successor document.

(b) GUIDANCE.—Not later than one year after the date of the enactment of this Act, the Director, in consultation with the Secretary of Defense, the National Cyber Director, the Director of National Intelligence, the Secretary of Homeland Security, and the head of any other department or agency the Director determines appropriate, shall issue guidance to facilitate the implementation of subsection (a), which shall include the following:

(1) Information regarding how departments and agencies are to utilize independent penetration test-

ing carried out by another department or agency, a national laboratory, or a private entity.

(2) Recommendations regarding how best to utilize, within the budget of an agency, penetration testing, including independent penetration testing.

(3) Recommendations for minimum rules of engagement.

(c) REPORT.—

(1) IN GENERAL.—Not later than one year after the date of the enactment of this Act, the Director shall submit to the appropriate congressional committees a report that includes the following:

(A) An analysis of whether increased engagement is needed from national laboratories and the private sector to assist with the protection of the information systems of agencies through the use of the following:

(i) Active defense techniques.

(ii) Deception technologies.

(iii) Penetration testing.

(B) An analysis of the feasibility and benefits of consolidating within the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security proactive cybersecurity initiatives.

(C) An analysis of whether the Director requires additional authorities or resources to carry out proactive cybersecurity initiatives for agencies.

(2) APPROPRIATE CONGRESSIONAL COMMITTEES DEFINED.—In this subsection, the term ''appropriate congressional committees'' means—

(A) with respect to the House of Representatives—

(i) the Committee on Appropriations;

(ii) the Committee on Armed Services;

(iii) the Committee on Homeland Security;

(iv) the Committee on the Judiciary;

(v) the Committee on Oversight and Reform; and

(vi) the Permanent Select Committee on Intelligence; and

(B) with respect to the Senate—

(i) the Committee on Appropriations;

(ii) the Committee on Armed Services;

(iii) the Committee on Homeland Security and Governmental Affairs;

(iv) the Committee on the Judiciary; and

(v) the Select Committee on Intelligence.

SEC. 4. STRENGTHENING THE OFFICE OF THE NATIONAL CYBER DIRECTOR.

(a) DECONFLICTION.—Section 1752(c)(1)(D) of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (6 U.S.C. 1500(c)(1)(D)) is amended—

(1) in clause (iii), by striking ''and'' at the end;

(2) in clause (iv), by inserting ''and'' at the end; and

(3) by adding at the end the following:

''(v) deconflicting overlapping jurisdiction between agencies regarding cybersecurity activities and authority to mitigate risks;''.

(b) INFORMATION SHARING.—Section 1752(c)(1) of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (6 U.S.C. 1500(c)(1)) is amended—

(1) in subparagraph (C)(vi), by inserting ''the Secretary of Homeland Security, the Director of the Office of Management and Budget,'' after ''the Assistant to the President for National Security Affairs,''; and

(2) in subparagraph (G), by inserting ''the Secretary of Homeland Security, the Director of the Office of Management and Budget, and'' after ''annually report to''.

SEC. 5. PENETRATION TESTING REPORTS.

(a) CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY.—

(1) AGGREGATION OF PENETRATION TESTING RESULTS.—Not later than one year after the date of the enactment of this Act and annually thereafter, the Director shall aggregate and review the results of the penetration testing provided to the Director under section 3(a)(1)(B).

(2) INTERAGENCY REPORTS.—Not later than 180 days after each review under paragraph (1), the Director, based on such review, shall provide to each agency a report containing the following:

(A) A summary of the results of such review, including an identification of risks and other results common across agencies.

(B) An assessment, based on the document entitled ''Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy'' (National Institute of Standards and

Technology Special Publication 800–37, Revision 2; December 2018) or a successor document, of the severity of risks identified under subparagraph (A).

(C) An analysis of the duration of time that such risks have existed.

(D) Recommendations for mitigating such risks, which prioritize risks assessed as the highest severity pursuant to subparagraph (B).

(3) CONGRESSIONAL REPORT.—Not later than 180 days after each report provided under paragraph (2), the Director shall submit to Congress a report that contains—

(A) a summary of the report provided under such paragraph; and

(B) recommendations for legislative action relating to the matters referred to in such paragraph.

(b) GOVERNMENT ACCOUNTABILITY OFFICE.—Not later than 180 days after the date of the enactment of this Act, the Comptroller General of the United States shall submit to Congress a report on penetration testing, which shall include the following:

(1) An identification of which departments or agencies are obligating and expending funds on pen-

etration testing and how such funds are being used, including whether such funds are being used on independent penetration testing.

(2) Recommendations for legislative action regarding additional authority or resources needed by departments or agencies to conduct penetration testing more effectively, including with respect to independent penetration testing.

SEC. 6. REPORT ON ACTIVE DEFENSE TECHNIQUES.

(a) REPORT.—Not later than 18 months after the date of the enactment of this Act, the Director, in consultation with the National Cyber Director and representatives of appropriate private sector entities, shall submit to the appropriate congressional committees a report regarding active defense techniques.

(b) CONTENTS.—The report described in subsection (a) shall include the following:

(1) An assessment of the effectiveness of active defense techniques to protect the information systems of departments or agencies.

(2) Recommendations regarding how such techniques can be better utilized to protect such systems, including best practices with respect to such techniques.

(3) An analysis of whether there are legislative, regulatory, or resource burdens that prevent such techniques from being effectively utilized, including the resources necessary to implement such techniques.

(4) An identification of resources necessary to carry out the recommendations under paragraph (2).

(5) An identification of other techniques that should be evaluated to protect such systems.

(c) APPROPRIATE CONGRESSIONAL COMMITTEES DEFINED.—In this subsection, the term ''appropriate congressional committees'' means—

(1) with respect to the House of Representatives—

(A) the Committee on Appropriations;

(B) the Committee on Armed Services;

(C) the Committee on Homeland Security;

(D) the Committee on the Judiciary;

(E) the Committee on Oversight and Reform; and

(F) the Permanent Select Committee on Intelligence; and

(2) with respect to the Senate—

(A) the Committee on Appropriations;

(B) the Committee on Armed Services;

(C) the Committee on Homeland Security and Governmental Affairs;

(D) the Committee on the Judiciary; and

(E) the Select Committee on Intelligence.

SEC. 7. STUDY ON INNOVATIVE USES OF PROACTIVE CYBERSECURITY INITIATIVES.

(a) STUDY.—The Secretary of Defense, in consultation with the Director of National Intelligence, the Secretary of Homeland Security, the Attorney General, and the head of any other department or agency the Director determines appropriate, shall conduct a study on innovative uses of proactive cybersecurity initiatives, including the following:

(1) The use of deception technologies.

(2) The use of continuous monitoring to generate evidence regarding how an information system—

(A) operates under normal or intended use; and

(B) behaves under a variety of adverse conditions or scenarios.

(3) The feasibility of department or agency adoption of a set of continuous monitoring procedures.

(b) REPORTS.—

(1) CLASSIFIED REPORT.—Not later than two years after the date of the enactment of this Act, the Secretary of Defense shall submit to the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate a classified report describing the results of the study required under subsection (a), including examples of any successes against attackers who unlawfully breached an information system of a department or agency.

(2) UNCLASSIFIED REPORT.—Not later than two years after the date of the enactment of this Act, the Secretary shall submit to the appropriate congressional committees an unclassified report describing the results of the study required under subsection (a), including legislative recommendations relating thereto.

(c) APPROPRIATE CONGRESSIONAL COMMITTEES DEFINED.—In this section, the term ''appropriate congressional committees'' means—

(1) with respect to the House of Representatives—

(A) the Committee on Armed Services;

(B) the Committee on Homeland Security;

(C) the Committee on the Judiciary;

(D) the Committee on Oversight and Reform; and

(E) the Permanent Select Committee on Intelligence; and

(2) with respect to the Senate—

(A) the Committee on Armed Services;

(B) the Committee on Homeland Security and Governmental Affairs;

(C) the Committee on the Judiciary; and

(D) the Select Committee on Intelligence.

○