SEC. 15___.[Log 74868] CYBER THREAT INFORMATION COLLABORATION ENVIRONMENT PROGRAM.

(a) PROGRAM.—Pursuant to the requirements established by the Cyber Threat Data Interoperability Council under subsection (c), the Secretary of Homeland Security shall develop an information collaboration environment consisting of a digital environment containing technical tools for information analytics and a portal through which relevant parties may submit and automate information inputs and access the environment to enable interoperable data flow that enables Federal and non-Federal entities to identify, mitigate, and prevent malicious cyber activity by—

(1) providing access to appropriate and operationally relevant data from unclassified and classified intelligence about cybersecurity risks and cybersecurity threats, as well as malware forensics and data from network sensor programs or network-monitoring programs, on a platform that enables querying and analysis;

(2) enabling cross-correlation of data on cybersecurity risks and cybersecurity threats at the speed and scale necessary for rapid detection and identification;

(3) facilitating a comprehensive understanding of cybersecurity risks and cybersecurity threats; and

(4) facilitating collaborative analysis between the Federal Government and public and private sector critical infrastructure entities and information sharing and analysis organizations.

(b) IMPLEMENTATION OF INFORMATION COLLABORATION ENVIRONMENT.—

(1) EVALUATION.—

(A) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Secretary of Homeland Security, acting through the Director of the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security, shall—

(i) identify, inventory, and evaluate existing Federal sources of classified and unclassified information on cybersecurity threats;

(ii) evaluate current programs, applications, or platforms intended to detect, identify, analyze, and monitor cybersecurity risks and cybersecurity threats;

(iii) consult with public and private sector critical infrastructure entities to

identify public and private critical infrastructure cyber threat capabilities, needs, and gaps; and

(iv) identify existing tools, capabilities, and systems that may be adapted to achieve the purposes of the information collaboration environment developed pursuant to subsection (a) to maximize return on investment and minimize cost.

(B) NATIONAL SECURITY SYSTEMS.—Nothing in this paragraph shall apply to a national security system, or to cybersecurity threat intelligence related to such systems, without the consent of the relevant element of the intelligence community.

(2) IMPLEMENTATION.—

(A) IN GENERAL.—Not later than one year after completing the evaluation required under paragraph (1)(A), the Secretary of Homeland Security, acting through the Director of the Cybersecurity and Infrastructure Security Agency, shall begin implementation of the information collaboration environment developed pursuant to subsection (a).

(B) REQUIREMENTS.—The information collaboration environment and the technical tools for information analytics under subsection (a) shall—

(i) operate in a manner consistent with relevant privacy, civil rights, and civil liberties policies and protections, including such policies and protections established pursuant to section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (6 U.S.C. 485);

(ii) reflect the requirements set forth by the Cyber Threat Data Interoperability Council under subsection (c);

(iii) enable integration of current applications, platforms, data, and information, including classified information, in a manner that supports the voluntary integration of unclassified and classified information on cybersecurity risks and cybersecurity threats;

(iv) incorporate tools to manage access to classified and unclassified data, as appropriate;

(v) ensure accessibility by Federal entities that the Secretary of Homeland Security, in consultation with the Director of National Intelligence, the Attorney General, and the Secretary of Defense, determines appropriate;

(vi) allow for access by public and private sector critical infrastructure entities and other private sector partners, at the discretion of the Secretary of Homeland Security and after consulting the appropriate Sector Risk Management Agency;

(vii) deploy analytic tools across classification levels to leverage all relevant data sets, as appropriate;

(viii) identify tools and analytical software that can be applied and shared to manipulate, transform, and display data and other identified needs; and

(ix) anticipate the integration of new technologies and data streams, including data from network sensor programs or network-monitoring programs deployed in support of non-Federal entities.

(C) ACCESS CONTROLS.—The owner of any data shared in the information collaboration environment shall have the authority to set access controls for such data and may restrict access to any particular data asset for any purpose, including for the purpose of protecting intelligence sources and methods from unauthorized disclosure in accordance with section 102A(i) of the National Security Act (50 U.S.C. 3024(i)).

(3) ANNUAL REPORT REQUIREMENT ON THE IMPLEMENTATION, EXECUTION, AND EFFECTIVENESS OF THE PROGRAM.—Not later than one year after the date of the enactment of this Act and annually thereafter, the Secretary of Homeland Security shall submit to the appropriate congressional committees a report that details—

(A) Federal Government participation in the information collaboration environment, including the Federal entities participating in the environment and the volume of information shared by Federal entities into the environment;

(B) non-Federal entities' participation in the information collaboration environment, including the non-Federal entities participating in the environment and the volume of information

shared by non-Federal entities into the environment;

(C) the impact of the information collaboration environment on positive security outcomes for the Federal Government and non-Federal entities;

(D) barriers identified to fully realizing the benefit of the information collaboration environment for both the Federal Government and non-Federal entities;

(E) additional authorities or resources necessary to successfully execute the information collaboration environment; and

(F) identified shortcomings or risks to data security and privacy, and the steps necessary to improve the mitigation of such shortcomings or risks.

(c) CYBER THREAT DATA INTEROPERABILITY COUNCIL.—

(1) ESTABLISHMENT.—There is established an interagency council, to be known as the ''Cyber Threat Data Interoperability Council'' (in this subsection referred to as the ''council''), chaired by the National Cyber Director, to establish data interoper-

ability requirements for data streams to be accessed in the information collaboration environment.

(2) MEMBERSHIP.—

(A) PRINCIPAL MEMBERS.—In addition to the National Cyber Director, the council shall have as its principal members the Secretary of Homeland Security, the Attorney General, the Director of National Intelligence, and the Secretary of Defense.

(B) ADDITIONAL FEDERAL MEMBERS.—Based on recommendations submitted by the principal members, the National Cyber Director shall identify and appoint council members from Federal entities that oversee programs that generate, collect, disseminate, or analyze data or information related to cybersecurity risks and cybersecurity threats.

(C) ADVISORY MEMBERS.—The National Cyber Director shall identify and appoint advisory members from non-Federal entities that shall advise the council based on recommendations submitted by the principal members.

(3) DATA STREAMS.—The council shall identify, designate, and periodically update programs that shall participate in or be interoperable with the in-

formation collaboration environment, which may include—

(A) network-monitoring and intrusion detection programs;

(B) cyber threat indicator sharing programs;

(C) certain network sensor programs or network-monitoring programs;

(D) incident response and cybersecurity technical assistance programs; or

(E) malware forensics and reverse-engineering programs.

(4) DATA PRIVACY.—The council shall establish a committee comprising privacy officers from the Department of Homeland Security, the Department of Justice, and the Office of the Director of National Intelligence to establish procedures and data governance structures, as necessary, to protect data shared in the information collaboration environment, comply with Federal regulations and statutes, and respect existing consent agreements with public and private sector critical infrastructure entities that apply to critical infrastructure information.

(5) RULE OF CONSTRUCTION.—Nothing in this subsection may be construed as changing existing

ownership or protection of, or policies and processes for access to, agency data.

(d) DEFINITIONS.—In this section:

(1) The term ''appropriate congressional committees'' means the following:

(A) The Committee on Homeland Security, the Committee on the Judiciary, the Committee on Armed Services, and the Permanent Select Committee on Intelligence of the House of Representatives.

(B) The Committee on Homeland Security and Governmental Affairs, the Committee on the Judiciary, the Committee on Armed Services, and the Select Committee on Intelligence of the Senate.

(2) The term ''critical infrastructure information'' has the meaning given such term in section 2222 of the Homeland Security Act of 2002 (6 U.S.C. 671).

(3) The term ''cyber threat indicator'' has the meaning given such term in section 102 of the Cybersecurity Act of 2015 (6 U.S.C. 1501).

(4) The term ''cybersecurity threat'' has the meaning given such term in section 102 of the Cybersecurity Act of 2015 (6 U.S.C. 1501).

(5) The term ''data asset'' has the meaning given such term in section 3502 of title 44, United States Code.

(6) The term ''environment'' means the information collaboration environment established under subsection (a).

(7) The term ''information sharing and analysis organization'' has the meaning given such term in section 2222 of the Homeland Security Act of 2002 (6 U.S.C. 671).

(8) The term ''intelligence community'' has the meaning given such term in section 3(4) of the National Security Act of 1947 (50 U.S.C. 3003(4)).

(9) The term ''national security system'' has the meaning given such term in section 3552 of title 44, United States Code.

(10) The term ''non-Federal entity'' has the meaning given such term in section 102 of the Cybersecurity Act of 2015 (6 U.S.C. 1501).

(11) The term ''Sector Risk Management Agency'' has the meaning given such term in section 2201 of the Homeland Security Act of 2002 (6 U.S.C. 651).