subsection (b) and notifications made under subsection (c); and

(B) in addition to the congressional defense committees, the Select Committee on Intelligence of the Senate, and the Permanent Select Committee on Intelligence of the House of Representatives with respect to—

(i) briefings required under subsection (b) regarding requirements of the intelligence community being incorporated into phase three planning; and

(ii) notifications made under subsection (c) regarding an assignment that includes capabilities being launched for the intelligence community.

(2) 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)).

(3) PHASE THREE.—The term ''phase three'' means, with respect to the National Security Space Launch program, launch missions ordered under the program after fiscal year 2024.

(4) PHASE TWO.—The term ''phase two'' means, with respect to the National Security Space Launch program, launch missions ordered under the program during fiscal years 2020 through 2024.

SA 6354. Mr. KING (for himself, Mr. SASSE, Ms. HASSAN, and Mr. OSSOFF) submitted an amendment intended to be proposed to amendment SA 5499 submitted by Mr. REED (for himself and Mr. INHOFE) and intended to be proposed to the bill H.R. 7900, to authorize appropriations for fiscal year 2023 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes; which was ordered to lie on the table; as follows:

At the appropriate place in subtitle G of title X, insert the following:

SEC. 10___. INFORMATION COLLABORATION ENVIRONMENT PROGRAM.

(a) DEFINITIONS.—In this section:

(1) COUNCIL.—The term ''Council'' means the Cyber Threat Data Collaboration Council established under subsection (d)(1).

(2) CRITICAL INFRASTRUCTURE.—The term ''critical infrastructure'' has the meaning given such term in section 1016(e) of the Critical Infrastructure Protection Act of 2001 (42 U.S.C. 5195c(e)).

(3) CRITICAL INFRASTRUCTURE INFORMATION.—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).

(4) CYBERSECURITY THREAT.—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) CYBER THREAT INDICATOR.—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).

(6) ENVIRONMENT.—The term ''environment'' means the information collaboration environment established under subsection (b).

(7) INFORMATION SHARING AND ANALYSIS ORGANIZATION.—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) NATIONAL INTELLIGENCE PROGRAM.—The term ''National Intelligence Program'' has the meaning given such term in section 3 of the National Security Act of 1947 (50 U.S.C. 3003).

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

(10) NON-FEDERAL ENTITY.—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) SECRETARY.—The term ''Secretary'' means the Secretary of Homeland Security.

(12) SECTOR RISK MANAGEMENT AGENCY.—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).

(13) UNITED STATES PERSON.—The term ''United States person'' has the meaning given that term in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801).

(b) INFORMATION COLLABORATION ENVIRONMENT.—In accordance with the requirements established by the Council under subsection (d), the Secretary, in coordination with the Secretary of Defense, acting through the Director of the National Security Agency (in the capacity of the Director as the National Manager for National Security Systems), shall ensure the development or establishment of an information collaboration environment, using existing programs and systems where available, through which relevant Federal entities and non-Federal entities may share information and collaborate to identify, mitigate, and prevent malicious cyber activity by—

(1) providing access to appropriate and operationally relevant data from unclassified and classified sources on cybersecurity threats, including malware forensics and data from network sensor programs, on a platform that enables query and analysis;

(2) enabling analysis of data on cybersecurity threats at the speed and scale necessary for rapid detection and identification of such threats, including through automated means where appropriate;

(3) facilitating a comprehensive understanding of 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, including by providing such entities and organizations access to the environment.

(c) IMPLEMENTATION OF ENVIRONMENT.—

(1) INVENTORY AND EVALUATION.—

(A) IN GENERAL.—Not later than 180 days after the date of enactment of this Act, the Secretary, in coordination with the Secretary of Defense, acting through the Director of the National Security Agency, shall conduct an inventory and evaluation of Federal programs and capabilities and submit to the Council a report that shall—

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

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

(iii) identify tools, capabilities, and systems that may be adapted to achieve the purposes of the environment in order to achieve a return on investment that is commensurate with the cost;

(iv) identify and evaluate interagency or public-private programs that may be adapted for, incorporated into, or accounted for in the design and implementation of the environment; and

(v) include a classified annex the contents of which shall be determined by the Director of the National Security Agency in coordination with the heads of Federal entities that own, operate, or control relevant national security systems, in accordance with paragraph (4).

(B) CONSULTATION.—In conducting the inventory and evaluation required under subparagraph (A), the Secretary, shall consult with—

(i) public and private sector critical infrastructure entities to identify public and private critical infrastructure cyber threat capabilities, needs, and gaps; and

(ii) the owners of Federal systems identified as part of the inventory.

(2) IMPLEMENTATION PLAN.—Not later than 180 days after the date on which the Secretary completes the inventory and evaluation under paragraph (1), the Secretary, in coordination with the Secretary of Defense, acting through the Director of the National Security Agency, shall submit to the Council for approval an implementation plan for the environment that—

(A) meets the requirements described in paragraph (3)(B);

(B) outlines roles and responsibilities of the Cybersecurity and Infrastructure Security Agency, the National Security Agency, and participating departments and agencies in the design, development, and operation of the environment;

(C) identifies programs to be included in the environment and their use and incorporation in the environment;

(D) describes application and design of access control mechanisms to ensure control of data by the applicable departments and agencies and the protection of privacy and classified or law enforcement sensitive information;

(E) identifies timelines for implementation;

(F) provides estimated costs for initial implementation and yearly operations and maintenance;

(G) provides estimated costs for participating departments and agencies in the maintenance or modernization of relevant programs and systems;

(H) establishes plans of action and milestones associated with achieving initial operating capability and full operating capability of the environment;

(I) identifies, assesses, and provides recommendations to address legal, policy, procedural, or budgetary challenges to implementation; and

(J) includes a classified annex that addresses any design or implementation issues related to the protection of intelligence sources and methods, and classified information and systems, as applicable and determined by the Director of the National Security Agency, in coordination with the heads of relevant Federal entities, in accordance with paragraph (4).

(3) IMPLEMENTATION.—

(A) IN GENERAL.—Not later than 180 days after the date of enactment of this Act, and after the Council approves the implementation plan required under paragraph (2), the Secretary, in coordination with the Secretary of Defense, acting through the Director of the National Security Agency, shall ensure initial operation capability of the environment and the ability of participants in the environment to develop and run analytic tools on specified data sets for the purpose of identifying cybersecurity threats.

(B) REQUIREMENTS.—The environment and the analytic tools used in the environment shall—

(i) operate in a manner consistent with applicable Federal security, privacy, civil rights, and civil liberties laws, policies and protections, including such policies and protections established pursuant to subsections (a)(4), (b), and (d)(5) of section 105 of the Cybersecurity Act of 2015 (6 U.S.C. 1504);

(ii) reflect the requirements set forth by Council;

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

(iv) incorporate tools to manage access to classified and unclassified data, as appropriate, for public and private sector personnel who are cleared for access to the highest level of classified data included in the environment;

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

(vi) allow for access by critical infrastructure stakeholders and other private sector partners, at the discretion of the Secretary, 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 sources, including data from appropriate Government-sponsored network sensors or network-monitoring programs deployed in support of non-Federal entities.

(C) ACCESS CONTROLS.—The owner or originator of any data that has been authorized to be shared in the environment by that owner or originator shall have the authority to set access controls for such data and may restrict access to any particular data for any purpose, including for the purposes of protecting classified information and intelligence sources and methods from unauthorized disclosure, in accordance with any applicable Executive Order or an Act of Congress (including section 102A(i) of the National Security Act (50 U.S.C. 3024(i))).

(4) NATIONAL SECURITY SYSTEMS.—

(A) IN GENERAL.—Subject to subparagraphs (B) and (C), nothing in this section shall apply to national security systems or to information related to such systems, without the consent of the Federal entity that owns, operates, or controls the relevant national security system.

(B) NATIONAL MANAGER INVENTORY.—The Director of the National Security Agency shall request all Federal entities that own, operate, or control a national security system to identify all national security systems with capabilities or functions that are relevant to the environment.

(C) NATIONAL MANAGER DETERMINATION.—The Director of the National Security Agency may include a national security system identified under subparagraph (B) in the inventory and evaluation under paragraph (1) and the environment, with the consent of the Federal entity that owns, operates, or controls the national security system.

(5) ANNUAL REPORT REQUIREMENT ON THE IMPLEMENTATION, EXECUTION, AND EFFECTIVENESS OF THE PROGRAM.—Not later than 1 year after the date of enactment of this Act, and every year thereafter, the Secretary, in coordination with the Secretary of Defense and the Director of National Intelligence, shall submit to the President, the Council, the Committee on Homeland Security and Governmental Affairs, the Committee on Armed Services, and the Select Committee on Intelligence of the Senate, and the Committee on Homeland Security, the Committee on Armed Services, and the Permanent Select Committee on Intelligence of the House of Representatives a report that details—

(A) Federal Government participation in the 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 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 environment on positive security outcomes for the Federal Government and non-Federal entities, such as owners of data that restrict access to particular data under paragraph (3)(C);

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

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

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

(d) CYBER THREAT DATA COLLABORATION COUNCIL.—

(1) ESTABLISHMENT.—There is established an interagency council, to be known as the ''Cyber Threat Data Collaboration Council'', which shall—

(A) ensure the implementation of the environment meets the requirements of this section;

(B) establish interoperability requirements for programs and systems participating or to be accessed in the environment;

(C) establish procedures, guidelines, and criteria for interagency cyber threat information sharing in the environment; and

(D) identify and work to address legal, policy, procedural, or technical barriers to ensure more effective and efficient interagency cyber threat information sharing and analysis in the environment.

(2) MEMBERSHIP.—

(A) PRINCIPAL MEMBERS.—The principal members of the Council shall be the National Cyber Director (who shall serve as the Chairperson of the Council), the Secretary, the Attorney General, the Director of National Intelligence, the Director of the National Security Agency, and the Secretary of Defense.

(B) ADDITIONAL FEDERAL MEMBERS.—The National Cyber Director shall identify and appoint additional members of the Council from among the heads of departments and agencies of Federal entities that oversee programs that generate, collect, disseminate, or analyze data or information on cybersecurity threats based on recommendations submitted by the principal members.

(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.

(D) TECHNICAL ADVISORS.—The National Cyber Director may identify and invite Federal employees with specific relevant experience, background, technical, or subject matter expertise to participate in the Council as technical advisors, based on recommendations submitted by the principal members.

(3) PARTICIPATING PROGRAMS.—

(A) INITIAL DETERMINATION.—Not later than 30 days after receiving the inventory and evaluation required under subsection (c), the Council shall, based on the results of the inventory and evaluation, approve an initial list of programs or classes of programs that shall be designated and required to participate in or be interoperable with the environment, which may include—

(i) endpoint detection and response, system monitoring and other intrusion detection, and prevention programs;

(ii) cyber threat indicator sharing programs;

(iii) appropriate Government-sponsored network sensors or network-monitoring programs;

(iv) incident response and cybersecurity technical assistance programs; and

(v) malware forensics and reverse-engineering programs.

(B) YEARLY REVIEW.—The Council shall conduct a yearly review of programs required to participate in or be interoperable with the environment and update the list of programs as appropriate.

(4) DATA PRIVACY AND CIVIL LIBERTIES.—The Council shall establish a committee comprised of privacy, civil liberties, and intelligence oversight officers from the Department of Homeland Security, the Department of Defense, the Department of Justice, and the Office of the Director of National Intelligence to advise the Council on matters related to procedures and data governance structures, as necessary, to protect data shared in the environment, comply with Federal regulations and statutes on using and storing the data of United States persons, and respect agreements with non-Federal entities concerning their information.

(5) RULE OF CONSTRUCTION.—Nothing in this subsection shall change existing ownership or protection of, or policies and processes for access to, agency data.

(e) DURATION.—The program under this section shall terminate on the date that is 5 years after the date on which the Secretary achieves initial operating capability of the program as required under subsection (c)(3).

(f) RESOURCES.—Subject to the availability of appropriations and under conditions established jointly by the Secretary and Secretary of Defense, in coordination with the Director of National Intelligence, and subject to the concurrence of the Director regarding the use of any funds made available under the National Intelligence Program, the National Security Agency shall provide to the Cybersecurity and Infrastructure Security Agency resources, personnel, expertise, infrastructure, equipment, or such other support as may be required in the design, development, maintenance, or operation of the environment.

(g) PROTECTION OF SOURCES AND METHODS.—Consistent with section 102A of the National Security Act of 1947 (50 U.S.C. 3024), the Director of National Intelligence shall ensure this section is implemented in a manner that protects intelligence sources and methods. Federal entities implementing the environment or participating in the activities described in this section shall follow applicable policy and guidance issued by the Director of National Intelligence regarding the protection of intelligence sources and methods.

SA 6355. Mr. KING (for himself and Mrs. FISCHER) submitted an amendment intended to be proposed to amendment SA 5499 submitted by Mr. REED (for himself and Mr. INHOFE) and intended to be proposed to the bill H.R. 7900, to authorize appropriations for fiscal year 2023 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes; which was ordered to lie on the table; as follows:

At the end of subtitle B of title XV, add the following: