H.R. 2500—FY20 NATIONAL DEFENSE AUTHORIZATION BILL

SUBCOMMITTEE ON INTELLIGENCE AND EMERGING THREATS AND CAPABILITIES

SUMMARY OF BILL LANGUAGE

Table Of Contents

DIVISION A—DEPARTMENT OF DEFENSE AUTHORIZATIONS

TITLE II—RESEARCH, DEVELOPMENT, TEST, AND EVALUATION

LEGISLATIVE PROVISIONS

SUBTITLE C—REPORTS AND OTHER MATTERS

Section 2xx—Diversification of the Science, Technology, Research, and Engineering Workforce of the Department of Defense

This section would require the Secretary of Defense to assess critical skillsets required in the Department of Defense's science, technology, research, and engineering workforce to support emerging and future warfighter technologies, to include an analysis of the recruiting, retention and representation of minorities and women in the current workforce.

Additionally, this section would require the Secretary of Defense to develop and implement a plan to diversify and strengthen the Department's science, technology, research, and engineering workforce using existing programs and authorities to include authorities granted in sections 2304d, 2371, and 2358 of title 10, United States Code.

Finally, this section would require the Secretary to submit a report to the congressional defense committees within 1 year from the date of the enactment of this Act with the plan to diversify the workforce.

Section 2xx—Master Plan for Implementation of Authorities Relating to Science and Technology Reinvention Laboratories

This section would require the Secretary of Defense, acting through the Under Secretary of Defense for Research and Engineering (USD(R&E)), to provide a master plan to the congressional defense committees by October 30, 2020, on how the Department of Defense will use its current authorities and responsibilities granted in previous National Defense Authorization Acts to modernize the workforce and capabilities of its science and technology reinvention laboratories. Further, this provision would require an initial report from USD(R&E) to be submitted to the congressional defense committees within 180 days after the date of the enactment of this Act on the barriers that prevent each military service from fully implementing currently available authorities and responsibilities. This section would direct the USD(R&E) to create the plan and report in consultation with the Secretary of each military department, the Service Acquisition Executives, and the affected commanders of each military command with responsibilities relating to research and engineering.

Section 2xx—Development and Implementation of Digital Engineering Capability and Automated Software Testing and Evaluation

This section would direct the Under Secretary of Defense for Research and Engineering and the Director, Operational Test and Evaluation, in consultation with Under Secretary of Defense for Acquisition and Sustainment, the military service acquisition executives, the service testing commands, and Defense Digital Service, to design, develop, and implement digital engineering capability and infrastructure to provide technically accurate digital models to the acquisition process that serve as the foundation for automated approaches to software testing and evaluation.

Additionally, this section would direct the Under Secretary and Director to carry out pilot programs to demonstrate whether it is possible for automated testing to satisfy developmental and operational test requirements to enable the Department to find and prevent defects in software earlier and deliver new capability to the field faster and on an iterative basis. This section would also direct the Under Secretary and Director to implement policies and guidance for both efforts and would require an initial report be submitted to the congressional defense committees outlining details on the selected pilot programs.

Section 2xx—Process to Align Policy Formulation and Emerging Technology Development

This section would direct the Secretary of Defense to establish a process to ensure that the policies of the Department of Defense relating to emerging technology are formulated and updated continuously as such technology is developed by the Department not later than 180 days after the date of the enactment of this Act. This section would also require the Secretary to submit a report on the process to the congressional defense committees.

The committee notes that technology development often outpaces policy formulation. For example, the Department is investing significantly in hypersonics, artificial intelligence, directed energy, and other cutting-edge technologies without a cohesive policy regarding development and employment of such capabilities, including the use of these technologies for offensive purposes. The committee believes the Department should better align policy formulation with technology development in order to promote responsible capability development and facilitate rapid and appropriate deployment to the warfighter.

Section 2xx—Biannual Report on the Joint Artificial Intelligence Center

This section would require a biannual report by the Secretary of Defense on the Joint Artificial Intelligence Center (JAIC) and its efforts to harmonize the Department's work on artificial intelligence (AI) issues. The report would require the Department to detail the status of the JAIC, its current staffing, hiring efforts, and investment priorities. The report would specify how the JAIC is working with

the military services, academia, industry, and international partners to develop and operationalize AI.

The committee supports the work of the Department of Defense on matters related to AI, as evident in section 238 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Public Law 115–232), which directed the establishment of a set of activities within the Department of Defense to coordinate the efforts of the Department to develop, mature, and transition artificial intelligence technologies into operational use. The committee will ensure that the Department approaches issues involving AI, such as workforce development and ethical use, in a substantive and comprehensive manner.

Section 2xx—Department-Wide Software Science and Technology Strategy

This section would require that the Secretary of Defense, acting through the Under Secretary of Defense for Research and Engineering, designate a senior official with principal responsibility for guiding the direction of research and development of next generation software and software intensive systems for the Department of Defense. Further, this section would require that the designated senior official develop a strategy for research and development of the next generation software and software intensive systems and submit the strategy to the congressional defense committees not later than 1 year after the date of the enactment of this Act.

Section 2xx—Master Plan for Infrastructure Required to Support Research, Development, Test, and Evaluation Missions

This section would require the Secretary of Defense, in consultation with the Secretaries of the military departments, to develop and implement a master plan that addresses the research, development, test, and evaluation infrastructure and modernization requirements of the Department of Defense, to include the science and technology reinvention laboratories and the Major Range and Test Facility Bases. This section would require the master plan be provided to the congressional defense committees by October 30, 2020.

The committee is aware that the laboratories and test facilities do not compete well across the military departments for military construction and other infrastructure funding and that authorities provided to promote and allow for infrastructure investment remain underutilized by the Department. The committee expects the Department to utilize authorities provided by Congress to ensure the in-house infrastructure of the Department remains viable in order to continue to support warfighter requirements.

In developing the master plan, the committee expects the Secretary to enlist the expertise of the Under Secretary of Defense for Research and Engineering, the Under Secretary of Defense for Acquisition and Sustainment, and the Director of Operational Test and Evaluation. Finally, the committee expects the Secretaries of the military departments to enlist the expertise of their Service Acquisition

Executives and civilian research leadership as well as the relevant commanders of each military command with responsibility for research and engineering.

Section 2xx—Program on Enhancement of Preparation of Dependents of Members of Armed Forces for Careers in Science, Technology, Engineering, and Mathematics

This section would make section 233 of the Carl Levin and Howard P. "Buck" McKeon National Defense Authorization Act for Fiscal Year 2015 (Public Law 113-291) permanent. Section 233 created a pilot program on enhancement of preparation of dependents of members of Armed Forces for careers in science, technology, engineering, and mathematics (STEM). The program improves STEM learning and performance for children; helps retain service members; provides STEM education opportunities to children in lower socioeconomic communities from which the U.S. military recruits heavily; and is a national level curriculum that works well for families that move around the country.

The committee expects the Secretary of Defense to continue to coordinate with other government organizations and departments as appropriate, to include the Secretary of Education, the National Science Foundation, and the heads of such other Federal, State, and local government and private sector organizations as the Secretary of Defense considers appropriate. Additionally, the committee expects the Secretary to continue, to the maximum extent practicable, to make use of the authorities under chapter 111 and sections 2601, 2605, and 2374a of title 10, United States Code, section 219 of the Duncan Hunter National Defense Authorization Act for Fiscal Year 2009 (10 U.S.C. 2358), and such other authorities as the Secretary of Defense considers appropriate.

Section 2xx—Grants for Civics Education Programs

This section would require that the Secretary of Defense carry out a program under which the Secretary makes grants to eligible entities, on a competitive basis, to support the development and evaluation of civics education programs.

Section 2xx—Strategy and Implementation Plan for Fifth Generation Information and Communications Technologies

This section would require the Secretary of Defense to develop and implement a strategy for fifth generation information and communications technologies not later than 270 days after the date of the enactment of this Act and to provide a briefing to the congressional defense committees not later than 180 days after the date of the enactment of this Act on progress in developing the strategy.

Section 2xx—Artificial Intelligence Education Strategy

This section would require the Secretary of Defense to develop a strategy which identifies the key aspects, applications, and challenges associated with artificial intelligence that can be developed into an educational curriculum for military service members who utilize the technology in the execution of responsibilities. This section would also require the development of an implementation plan for the educational curriculum, and mandates that the Department of Defense provide the Artificial Intelligence Education Strategy and the associated implementation plan to the congressional defense committees not later than 270 days after the date of the enactment of this Act.

TITLE VIII—ACQUISITION POLICY, ACQUISITION MANAGEMENT, AND RELATED MATTERS

LEGISLATIVE PROVISIONS

SUBTITLE F—OTHER MATTERS

Section 8xx—Extension of Sunset Relating to Federal Data Center Consolidation Initiative

This section would extend the sunset date of the Federal Data Center Consolidation Initiative established in section 834 of the Carl Levin and Howard P. "Buck" McKeon National Defense Authorization Act for Fiscal Year 2015 (Public Law 113–291) from October 1, 2020, to October 1, 2022.

TITLE X—GENERAL PROVISIONS

LEGISLATIVE PROVISIONS

SUBTITLE A—FINANCIAL MATTERS

Section 10xx—Annual Budget Justification Display for Service-Common and Other Support and Enabling Capabilities for Special Operations Forces

This section would require the Secretary of Defense to provide a consolidated budget display to Congress annually as part of the President's budget request showing service-common and other support and enabling capabilities for special operations forces (SOF) requested by a military service or defense agency.

The committee appreciates the level of fidelity provided in the budget request for Major Force Program (MFP)-11 administered by U.S. Special Operations Command for SOF-peculiar and command-specific programs, activities, and services. The budget request contained $13.8 billion in MFP-11 which accounts for 2 percent of the total budget request for the Department. According to the Department, service-common support and enabling capabilities requested by the

military departments for SOF contained in the budget request is approximately $8.0 billion, bringing the total amount requested for SOF to more than $21.0 billion. However, the committee is aware that other elements of the Department, such as the Defense Threat Reduction Agency, Combating Terrorism and Technical Support Office, and Defense Innovation Unit also request and expend funds to support SOF that may not be reflected in the service-common total. Therefore, the committee requires a better understanding of the total amounts requested for SOF across the Department and greater consolidated detail on such service-common and other enabling capabilities and support requested each fiscal year.

SUBTITLE E—MISCELLANEOUS AUTHORITIES AND LIMITATIONS

Section 10xx—Notification on the Provision of Defense Sensitive Support

This section would modify section 1055 of the National Defense Authorization Act for Fiscal Year 2017 (Public Law 114-328) to provide additional Defense Sensitive Support reporting requirements.

Section 10xx—Extension of National Security Commission on Artificial Intelligence

This section would modify reporting requirements for the National Security Commission on Artificial Intelligence, as established in section 1051 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Public Law 115-232) by 180 days and extend the termination date to March 1, 2021.

SUBTITLE F—STUDIES AND REPORTS

Section 10xx—Annual Report on Joint Military Information Support Operations Web Operations Center

This section would require the Commander of U.S. Special Operations Command (SOCOM) to provide an annual report to the congressional defense committees not later than December 1 of each year on the Joint Military Information Support Operations (MISO) Web Operations Center (JMWC). The report shall include a description of MISO activities hosted by the JMWC, activities conducted to achieve initial operating capability and full operational capability, measures of effectiveness, infrastructure, leveraging lessons learned across the platform, number of personnel, and synchronization of efforts across the interagency and with international partners, as appropriate.

The committee supports efforts to improve the effectiveness and efficiency of MISO programs. However, the committee is concerned the current plan for establishment of the JMWC is focused on consolidation rather than efficiencies and lacks focus on efforts to leverage lessons learned and implement measures of effectiveness across the geographic combatant commands.

Section 10xx—Assessment of Special Operations Force Structure

This section would require the Secretary of Defense to enter into an agreement with a federally funded research and development center for the conduct of an independent assessment of the force structure and roles and responsibilities of special operations forces and to submit the assessment to the congressional defense committees not later than July 1, 2020.

SUBTITLE G—OTHER MATTERS

Section 10xx—Processes and Procedures for Notifications regarding Special Operations Forces

This section would mandate the Secretary of Defense establish and submit processes and procedures for providing notifications to the congressional defense committees regarding members of special operations forces. This section would also mandate that the processes and procedures include clarification of the roles and responsibilities of the Secretaries of the military departments, the Assistant Secretary of Defense for Special Operations and Low Intensity Conflict, and the Commander of U.S. Special Operations Command in providing such notifications to Congress.

The Secretaries of the military departments provide notification to the congressional defense committees regarding members of the Armed Forces who receive awards of valor, demonstrate acts of heroism, are killed or wounded in action or while on duty, are alleged to have committed serious offenses punishable under the Uniform Code of Military Justice, are involved in high-profile incidents, and for other matters of interest.

However, the committee notes that ambiguity regarding the roles and responsibilities of the Secretaries of the military departments, the Commander of U.S. Special Operations Command, and the Assistant Secretary of Defense for Special Operations and Low Intensity Conflict relating to notifications involving special operations forces have resulted in inconsistent, or lack of, notifications. For example, the congressional defense committees were not provided notifications of reprimands issued as a result of the investigation into the incident in Niger in 2017.

The committee expects processes and procedures established under this provision to be consistent with the processes for notifications involving the conventional forces and to account for the privacy of members of the Armed Forces.

TITLE XII—MATTERS RELATING TO FOREIGN NATIONS

LEGISLATIVE PROVISIONS

SUBTITLE F—OTHER MATTERS

Section 12xx—Extension and Modification of NATO Special Operations Headquarters

This section would extend the funding authority granted in section 1244 of the National Defense Authorization Act for Fiscal Year 2010 (Public Law 111-84) for NATO Special Operations Headquarters (NSHQ) through fiscal year 2023. This section would also establish an annual reporting requirement on activities conducted by NSHQ and includes a limitation on funding until the Assistant Secretary of Defense for Special Operations and Low Intensity Conflict provides a report to the congressional defense committees on the 2019 rearrangement of responsibilities for overseeing and supporting NSHQ.

TITLE XVI—STRATEGIC PROGRAMS, CYBER, AND INTELLIGENCE MATTERS

LEGISLATIVE PROVISIONS

SUBTITLE B—DEFENSE INTELLIGENCE AND INTELLIGENCE-RELATED ACTIVITIES

Section 16xx—Survey and Report on Alignment of Intelligence Collections Capabilities and Activities with Department of Defense Requirements

This section would require the Under Secretary of Defense for Intelligence, in coordination with the Chairman of the Joint Chiefs of Staff and the Director of National Intelligence, to review and provide a report to the congressional defense committees and the congressional intelligence committees, not later than 120 days after the date of the enactment of this Act, on the organization, posture, and processes of intelligence collections capabilities and activities, for the purpose of assessing the ability of the intelligence collections capabilities and activities to support the current and future requirements of the Department of Defense.

Section 16xx—Modifications to ISR Integration Council and Annual Briefing Requirements

This section would amend section 426 of title 10, United States Code, to modify council membership and annual briefing requirements of the Intelligence, Surveillance, and Reconnaissance Integration Council in the Department of Defense.

SUBTITLE C—CYBERSPACE-RELATED MATTERS

Section 16xx—Notification Requirements for Sensitive Military Cyber Operations

This section would modify section 395 of title 10, United States Code, which requires the Secretary of Defense to provide notification of sensitive military cyber operations to the congressional defense committees. The modifications include additional parameters to further define what offensive and defensive operations constitute a sensitive military cyber operation in order to strengthen oversight.

The committee recognizes that the Department of Defense has implemented section 395 of title 10, United States Code. However, the committee notes that the Department's definition of and threshold for sensitive military cyber operations notifications is not aligned with the intent of the committee. As military cyber operations increase in frequency and scope, the committee expects to be continually notified and kept fully and currently informed, in order to conduct oversight.

Section 16xx—Tier 1 Exercise of Support to Civil Authorities for a Cyber Incident

This section would revise section 1648 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Public Law 115-232) by directing the Commanders of U.S. Northern Command and U.S. Cyber Command to conduct a Tier 1 exercise by February 1, 2020. This section would also place a limitation on 10 percent of fiscal year 2020 funds authorized to be appropriated for the White House Communications Agency until the exercise is initiated. Despite legislation directing the exercise in Public Law 115-232, the Department of Defense was unable to perform the exercise within fiscal year 2019, and the committee is concerned that the Department may not be focused adequately on the potential for a domestic cyber attack necessitating defense support to civil authorities.

Section 16xx—Extension of the Cyberspace Solarium Commission

This section would extend the Cyberspace Solarium Commission, as established in the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Public Law 115-232) and its final report by 1 year, from September 1, 2019, to September 1, 2020.

The committee notes that the Cyberspace Solarium Commission's work on developing a consensus on a strategic approach to defending the United States in cyberspace against cyber attacks of significant consequences would benefit from the inclusion of commissioners from the private sector who are able to represent the owners and operators of critical infrastructure, particularly the telecommunications, electricity, and financial sectors. These sectors have collaborated closely with government through the public-private partnership forum known as the Tri-Sector Executive Working Group.

Section 16xx—Notification of Delegation of Authorities to the Secretary of Defense for Military Operations in Cyberspace

This section would require the Secretary of Defense to notify the congressional defense committees within 15 days of any delegation of authorities from the National Command Authority for military cyberspace operations.

Section 16xx—Annual Military Cyberspace Operations Report

This section would require the Secretary of Defense to provide to the congressional defense committees, not later than March 1 of each calendar year, an annual report on military cyberspace operations, to include cyber effects enabling and cyber effects operations, activities, and missions.

The congressional defense committees do not receive written reports from the Department of Defense with details regarding military cyberspace operations. As military cyberspace operations mature, the committee expects to be kept fully apprised of operations, activities, and missions to include increasing fidelity on associated resources, units, tools, and infrastructure.

Section 16xx—Report on Synchronization of Efforts Relating to Cybersecurity in the Defense Industrial Base

This section would require the Secretary of Defense to provide a report to the congressional defense committees not later than May 1, 2020, on the Department of Defense's many efforts related to cybersecurity and the Defense Industrial Base. The committee supports efforts to improve cybersecurity across the Defense Industrial Base, both through efforts by the Department and amongst industry. The committee recognizes the Department's efforts to address the protection of Department information held outside of government networks, and is aware of many programs across various elements of the Department of Defense to assist vendors and contractors. However, the committee is concerned that these efforts are not coordinated or deconflicted. The committee is also concerned by the sense of confusion generated by either varying or contradictory regulatory requirements around cybersecurity, and even conflicting definitions of key terms such as "Controlled Unclassified Information" and "For Official Use Only."

To address these deficiencies, the committee mandates a report that would have the Department comprehensively identify all disparate programs that aim to assist the Defense Industrial Base with cybersecurity and cybersecurity compliance. Moreover, the report would identify potential overlaps in program objectives, the requisite resources needed to ensure objectives are achieved, and identify incongruous regulations and standards across the entire defense enterprise that should be harmonized. The Department would also need to clarify overlap in the cybersecurity responsibilities of the Under Secretary of Defense for Acquisition and Sustainment, the Chief Information Officer, the Chief Management Officer, the Director of the Protecting Critical Technologies Task Force, and the Secretaries of the military services.

Section 16xx—Evaluation of Cyber Vulnerabilities of Major Weapon Systems of the Department of Defense

This section would modify section 1647 of the National Defense Authorization Act for Fiscal Year 2016 (Public Law 114-92), that required evaluations of cyber vulnerabilities of each major weapon system of the Department of Defense by December 31, 2019, by requiring notification and justification for not meeting the deadline. Further, this section would require a comprehensive report from the Secretary of Defense, acting through the Under Secretary of Defense for Acquisition and Sustainment, upon completion of the requirement for evaluations of cyber vulnerabilities for each major weapon system to include vulnerabilities identified requiring mitigation, mitigation efforts, leveraging lessons learned across the Department, and incorporation of lessons learned to address or mitigate the likelihood of cyber vulnerabilities in major weapon systems through education and other changes earlier in the research, development, and acquisition cycle.

The committee commends the effort of the Department to meet the requirements of section 1647 of Public Law 114-92 and appreciates the Department's recognition that cyber vulnerabilities identified may not only require software or hardware solutions, but changes in doctrine, organization, training, materiel, leadership and education, personnel, and facilities to provide for comprehensive cybersecurity of weapon systems and prepare forces to operate in a cyber contested environment. However, the committee understands that not all organizations and entities, such as U.S. Special Operations Command, are aware of this effort and believes that lessons learned should be shared enterprise-wide. Thus, the committee requires a better understanding of vulnerabilities identified and joint solutions, as well as how lessons learned are being leveraged, shared, and institutionalized across the Department.

Finally, fidelity from the Department on resources relating to the evaluations and mitigation efforts requires improvement. Thus, the committee expects the Department to comply with section 1637 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Public Law 115-232) requiring a budget display relating to ongoing cyber vulnerability evaluations and mitigation efforts beginning with the fiscal year 2021 budget submission.

Section 16xx—Briefings on the Status of the National Security Agency and United States Cyber Command Partnership

This section would direct the Secretary of Defense to provide quarterly briefings to the congressional defense committees and congressional intelligence committees on the nature of the National Security Agency and United States Cyber Command current and future partnership. The quarterly briefing mandate would terminate on January 1, 2022.

Section 16xx—Limitation of Funding for Consolidated Afloat Networks and Enterprise Services

This section would place a limitation on 15 percent of all funds authorized to be appropriated by this Act for the Department of the Navy's Consolidated Afloat Networks and Enterprise Services until the Secretary of Defense certifies to the congressional defense committees that the Navy has implemented the recommendations of the Office of the Inspector General's audit of the program.

Section 16xx—Quarterly Cyber Operations Briefings

This section would modify section 484 of title 10, United States Code, to require an overview of the readiness of the Cyber Mission Force to be presented as part of the mandatory cyber operations quarterly briefings.

BILL LANGUAGE

SEC. 2___[Log 69202]. DIVERSIFICATION OF THE SCIENCE, TECHNOLOGY, RESEARCH, AND ENGINEERING WORKFORCE OF THE DEPARTMENT OF DEFENSE.

(a) ASSESSMENT REQUIRED.—

(1) IN GENERAL.—The Secretary of Defense, acting through the Under Secretary of Defense for Research and Engineering, shall conduct an assessment of critical skillsets required across the science, technology, research, and engineering workforce of the Department of Defense to support emerging and future warfighter technologies.

(2) ELEMENTS.—The assessment required by paragraph (1) shall include analysis of the following:

(A) The percentage of women and minorities employed in the workforce as of the date of the assessment.

(B) The percentage of grants, fellowships, and funding awarded to minorities and women.

(C) The effectiveness of existing hiring and attraction incentives, other encouragements, and required service agreement commitments in attracting and retaining minorities and women in the workforce of the Department after such

individuals complete work on Department-funded research projects, grant projects, fellowships, and STEM programs.

(b) PLAN REQUIRED.—

(1) IN GENERAL.—Based on the results of the assessment conducted under subsection (a), the Secretary of Defense, acting through the Under Secretary of Defense for Research and Engineering, shall develop and implement a plan to diversify and strengthen the science, technology, research, and engineering workforce of the Department of Defense.

(2) ELEMENTS.—The plan required by paragraph (1) shall—

(A) align with science and technology strategy priorities of the Department of Defense, including the emerging and future warfighter technology requirements identified by the Department;

(B) except as provided in subsection (c)(2), set forth steps for the implementation of each recommendation included in the 2013 report of the RAND corporation titled ''First Steps Toward Improving DoD STEM Workforce Diversity'';

(C) harness the full range of the Department's STEM programs and other Department-sponsored programs to develop and attract top talent;

(D) use existing authorities to attract and retain students, academics, and other talent;

(E) establish and use contracts, agreements, or other arrangements with institutions of higher education (as defined in section 101 of the Higher Education Act of 1965 (20 U.S.C. 1001)), including historically black colleges and universities and other minority-serving institutions (as described in section 371(a) of such Act (20 U.S.C. 1067q(a)) to enable easy and efficient access to research and researchers for government-sponsored basic and applied research and studies at each institution, including contracts, agreements, and other authorized arrangements such as those authorized under—

(i) section 217 of the National Defense Authorization Act for Fiscal Year 2018 (Public Law 115–91; 10 U.S.C. 2358 note); and

(ii) such other authorities as the Secretary determines to be appropriate; and

(F) include recommendations for changes in authorities, regulations, policies, or any other relevant areas, that would support the achievement of the goals set forth in the plan.

(3) SUBMITTAL TO CONGRESS.—Not later than one year after the date of the enactment of this Act, the Secretary of Defense shall submit to the congressional defense committees a report that includes—

(A) the plan developed under paragraph (1); and

(B) with respect to each recommendation described in paragraph (2)(B) that the Secretary implemented or expects to implement—

(i) a summary of actions that have been taken to implement the recommendation; and

(ii) a schedule, with specific milestones, for completing the implementation of the recommendation.

(c) DEADLINE FOR IMPLEMENTATION.—

(1) IN GENERAL.—Except as provided in paragraph (2), not later than 18 months after the date

of the enactment of this Act the Secretary of Defense shall carry out activities to implement the plan developed under subsection (b).

(2) EXCEPTION FOR IMPLEMENTATION OF CERTAIN RECOMMENDATIONS.—

(A) DELAYED IMPLEMENTATION.—The Secretary of Defense may commence implementation of a recommendation described in subsection (b)(2)(B) after the date specified in paragraph (1) if the Secretary provides the congressional defense committees with a specific justification for the delay in implementation of such recommendation on or before such date.

(B) NONIMPLEMENTATION.—The Secretary of Defense may opt not to implement a recommendation described in subsection (b)(2)(B) if the Secretary provides to the congressional defense committees, on or before the date specified in paragraph (1)—

(i) a specific justification for the decision not to implement the recommendation; and

(ii) a summary of the alternative actions the Secretary plans to take to ad-

dress the issues underlying the recommendation.

(d) STEM DEFINED.—In this section, the term ''STEM'' means science, technology, engineering, and mathematics.

SEC. 2___[Log 69247]. MASTER PLAN FOR IMPLEMENTATION OF AUTHORITIES RELATING TO SCIENCE AND TECHNOLOGY REINVENTION LABORATORIES.

(a) PLAN REQUIRED.—The Secretary of Defense, acting through the Under Secretary of Defense for Research and Engineering, shall develop a master plan for using current authorities and responsibilities to strengthen and modernize the workforce and capabilities of the science and technology reinvention laboratories of the Department of Defense (referred to in this section as the ''laboratories'') to enhance the ability of the laboratories to execute missions in the most efficient and effective manner.

(b) ELEMENTS.—The master plan required under subsection (a) shall include, with respect to the laboratories, the following;

(1) A summary of hiring and staffing deficiencies at laboratories, by location, and the effect of such deficiencies on the ability of the laboratories—

(A) to meet existing and future requirements of the Department of Defense; and

(B) to recruit and retain qualified personnel.

(2) A summary of existing and emerging military research, development, test, and evaluation mission areas requiring the use of the laboratories.

(3) An explanation of the laboratory staffing capabilities required for each mission area identified under paragraph (2).

(4) Identification of specific projects, including hiring efforts and management reforms, that will be carried out—

(A) to address the deficiencies identified in paragraph (1); and

(B) to support the existing and emerging mission areas identified in paragraph (2);

(5) For each project identified under paragraph (4)—

(A) a summary of the plan for the project;

(B) an explanation of the level of priority that will be given to the project; and

(C) a schedule of required investments that will be made as part of the project.

(6) A description of how the Department, including each military department concerned, will carry out the projects identified in paragraph (3) using—

(A) current authorities and responsibilities; and

(B) such other authorities as are determined to be relevant by the Secretary of Defense.

(7) Identification of any statutory barriers to implementing the master plan and legislative proposals to address such barriers.

(c) CONSULTATION.—In developing the master plan required under subsection (a), the Secretary of Defense and the Under Secretary of Defense for Research and Engineering shall consult with—

(1) the Secretary of each military department;

(2) the Service Acquisition Executives with responsibilities relevant to the laboratories;

(3) the commander of each military command with responsibilities relating to research and engineering that is affected by the master plan; and

(4) any other officials determined to be relevant by the Secretary of Defense and the Under Secretary of Defense for Research and Engineering

(d) INITIAL REPORT.—Not later than 180 days after the date of the enactment of this Act, the Under Secretary of Defense for Research and Engineering shall submit to the congressional defense committees a report that identi-

fies any barriers that prevent the full use and implementation of current authorities and responsibilities and such other authorities as are determined to be relevant by the Secretary of Defense, including any barriers presented by the policies, authorities, and activities of—

(1) organizations and elements of the Department of Defense; and

(2) organizations outside the Department.

(e) FINAL REPORT.—Not later than October 30, 2020, the Under Secretary of Defense for Research and Engineering shall submit to the congressional defense committees—

(1) the master plan developed under subsection (a); and

(2) a report on the activities carried out under this section.

SEC. 2___[Log 69249]. DEVELOPMENT AND IMPLEMENTATION OF DIGITAL ENGINEERING CAPABILITY AND AUTOMATED SOFTWARE TESTING AND EVALUATION.

(a) CAPABILITY REQUIRED.—

(1) IN GENERAL.—The Under Secretary of Defense for Research and Engineering and the Director of Operational Test and Evaluation shall jointly design, develop, and implement a digital engineering capability and infrastructure—

(A) to provide technically accurate digital models to the acquisition process; and

(B) to serve as the foundation for automated approaches to software testing and evaluation.

(2) ELEMENTS.—The capability developed under subsection (a) shall consist of digital platforms that may be accessed by individuals throughout the Department who have responsibilities relating to the development, testing, evaluation, and operation of software. The platforms shall enable such individuals to—

(A) use systems-level digital representations and simulation environments;

(B) perform automated software testing based on criteria developed, in part, in consultation with the Under Secretary's developmental test organization and the Director to satisfy program operational test requirements; and

(C) perform testing on a repeatable, frequent, and iterative basis.

(b) PILOT PROGRAMS.—

(1) IN GENERAL.—The Under Secretary and Director shall carry out pilot programs to demonstrate whether it is possible for automated testing to satisfy—

(A) developmental test requirements for the software-intensive programs of the Department of Defense; and

(B) the Director's operational test requirements for such programs.

(2) NUMBER OF PILOT PROGRAMS.—The Under Secretary and Director shall carry out not fewer than four and not more than ten pilot programs under this section.

(3) REQUIREMENTS.—For each pilot program carried out under paragraph (1), the Under Secretary and Director shall—

(A) conduct a cost benefit analysis that compares the costs and benefits of the digital engineering and automated testing approach of the pilot program to the non-digital engineering based approach typically used by the Department of Defense;

(B) ensure that the intellectual property strategy for the pilot program supports the data required to operate the models used under the program; and

(C) develop a workforce and infrastructure plan to support any new policies and guidance implemented during the pilot program or after the completion of the program.

(4) CONSIDERATIONS.—In carrying out paragraph (1), the Under Secretary and Director may consider using the authorities provided under sections 873 and 874 of the National Defense Authorization Act for Fiscal Year 2018 (Public Law 115–91).

(5) REPORT.—Not later than 90 days after the date of the enactment of this Act, the Under Secretary and Director shall submit to the congressional defense committees a report that includes a description of—

(A) each pilot program that will be carried out under paragraph (1);

(B) software programs that may be used as part of each pilot program;

(C) selection criteria and intellectual property and licensing issues relating to such software programs;

(D) any recommendations for changes to existing law to facilitate the implementation of the pilot programs; and

(E) such other matters as the Under Secretary and Director determine to be relevant.

(6) TERMINATION.—Each pilot program carried out under paragraph (1) shall terminate not later than December 31, 2025.

(c) POLICIES AND GUIDANCE REQUIRED.—

(1) IN GENERAL.—The Under Secretary and the Director shall issue policies and guidance to implement—

(A) the digital engineering capability and infrastructure developed under subsection (a); and

(B) the pilot programs carried out under subsection (b).

(2) ELEMENTS.—The policies and guidance issued under paragraph (1) shall—

(A) specify procedures for developing and maintaining digital engineering models and the automated testing of software throughout the program life cycle;

(B) include processes for automated testing of developmental test requirements and operational test requirements;

(C) include processes for automated security testing, including—

(i) penetration testing; and

(ii) vulnerability scanning;

(D) include processes for security testing performed by individuals, including red team assessments with zero-trust assumptions;

(E) encourage the use of an automated testing capability instead of acquisition-related processes that require artifacts to be created for acquisition oversight but are not used as part of the engineering process;

(F) support the high-confidence distribution of software to the field on a time bound, repeatable, frequent, and iterative basis;

(G) provide technically accurate models, including models of system design and performance, to the acquisition process; and

(H) ensure that models are continually updated with the newest design, performance, and testing data.

(d) CONSULTATION.—In carrying out subsections (a) through (c), the Under Secretary and Director shall consult with—

(1) the Under Secretary of Defense for Acquisition and Sustainment;

(2) the service acquisition executives;

(3) the service testing commands; and

(4) the Defense Digital Service.

(e) REPORT REQUIRED.—Not later one year after the date of the enactment of this Act, the Under Secretary and Director shall submit to the congressional defense committees a report on the progress of the Under Secretary and Director in carrying out subsections (a) through (c). The report shall include—

(1) an independent assessment conducted by the Defense Innovation Board of the progress made as of the date of the report;

(2) an explanation of how the results of the pilot programs carried out under subsection (b) will

inform subsequent policy and guidance, particularly the policy and guidance of the Director of Operational Test and Evaluation; and

(3) any recommendations for changes to existing law to facilitate the implementation of subsections (a) through (c).

(f) DEFINITIONS.—In this section:

(1) The term ''Under Secretary and Director'' means the Under Secretary of Defense for Research and Engineering and the Director of Operational Test and Evaluation, acting jointly.

(2) The term ''digital engineering'' means an integrated digital approach that uses authoritative sources of system data and models as a continuum across disciplines to support life-cycle activities from concept through disposal.

(3) The term ''zero-trust assumption'' means a security architecture philosophy designed to prevent all threats, including insider threats and outsider threats.

(4) The term ''red team assessment'' means penetration tests and operations performed on a system to emulate a capable adversary to expose security vulnerabilities.

SEC. 2___[Log 69250]. PROCESS TO ALIGN POLICY FORMULATION AND EMERGING TECHNOLOGY DEVELOPMENT.

(a) ALIGNMENT OF POLICY AND TECHNOLOGICAL DEVELOPMENT.—Not later than 180 days after the date of the enactment of this Act, the Secretary of Defense shall establish a process to ensure that the policies of the Department of Defense relating to emerging technology are formulated and updated continuously as such technology is developed by the Department.

(b) ELEMENTS.—As part of the process established under subsection (a), the Secretary shall—

(1) specify the role of each covered official in ensuring that the formulation of policies relating to emerging technology is carried out concurrently with the development of such technology;

(2) establish mechanisms to ensure that the Under Secretary of Defense for Policy has the information and resources necessary to continuously formulate and update policies relating to emerging technology, including by directing the organizations and entities of the Department of Defense responsible for the development such technology—

(A) to share information with the Under Secretary;

(B) to communicate plans for the fielding and use of emerging technology to the Under Secretary; and

(C) to coordinate activities relating to such technology with the Under Secretary; and

(3) incorporate procedures for the legal review of—

(A) weapons that incorporate emerging technology; and

(B) treaties that may be affected by such technology.

(c) REPORTS REQUIRED.—

(1) INTERIM REPORT.—Not later than 60 days after the date of the enactment of this Act, the Secretary of Defense shall submit to the congressional defense committees a report on the progress of the Secretary in carrying out subsection (a).

(2) FINAL REPORT.—Not later than 30 days after date on which the Secretary of Defense establishes the process required under subsection (a), the Secretary shall submit to the congressional defense committees a report that describes such process.

(d) DEFINITIONS.—In this section:

(1) The term ''covered official'' means the Chairman of the Joint Chiefs of Staff, the Under Secretary of Defense for Research and Engineering, the Under Secretary of Defense for Policy, the commanders of the combatant commands, and the Secretaries of the military departments.

(2) The term ''emerging technology'' means technology determined to be in an emerging phase of development by the Secretary of Defense and includes quantum computing, technology for the analysis of large and diverse sets of data (commonly known as ''big data analytics''), artificial intelligence, autonomous technology, robotics, directed energy, hypersonics, and biotechnology.

SEC. 2___[Log 69255]. BIANNUAL REPORT ON THE JOINT ARTIFICIAL INTELLIGENCE CENTER.

(a) REPORT.—Not later than 90 days after the date of the enactment of this Act and biannually thereafter through the end of 2023, the Secretary of Defense shall submit to the congressional defense committees a report on the Joint Artificial Intelligence Center (referred to in this section as the ''Center'').

(b) ELEMENTS.—Each report under subsection (a) shall include the following:

(1) Information relating to the mission and objectives of the Center.

(2) A description of the National Mission Initiatives, Component Mission Initiatives, and any other initiatives of the Center, including a description of—

(A) the activities carried out under the initiatives;

(B) any investments made or contracts entered into under the initiatives; and

(C) the progress of the initiatives.

(3) A description of how the Center has sought to leverage lessons learned, share best practices, avoid duplication of efforts, and transition artificial

intelligence research efforts into operational capabilities by—

(A) collaborating with other organizations and elements of the Department of Defense, including the Defense Agencies and the military departments; and

(B) deconflicting the activities of the Center with the activities of other organizations and elements of the Department.

(4) A description any collaboration between—

(A) the Center and the private sector and academia; and

(B) the Center and international allies and partners.

(5) The total number of military, contractor, and civilian personnel who are employed by the Center, assigned to the Center, and performing functions in support of the Center.

(6) A description of the organizational structure and staffing of the Center.

(7) A detailed description of the frameworks, metrics, and capabilities established to measure the effectiveness of the Center and the Center's investments in the National Mission Initiatives and Component Mission Initiatives.

(8) A description of any new policies, standards, or guidance relating to artificial intelligence that have been issued by the Chief Information Officer of the Department.

(c) JOINT ARTIFICIAL INTELLIGENCE CENTER DEFINED.—In this section, the term ''Joint Artificial Intelligence Center'' means the Joint Artificial Intelligence Center of the Department of Defense established pursuant to section 238 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Public Law 115–232).

SEC. 2___[Log 69261]. DEPARTMENT-WIDE SOFTWARE SCIENCE AND TECHNOLOGY STRATEGY.

(a) DESIGNATION OF SENIOR OFFICIAL.—Not later than 180 days after the date of the enactment of this Act, the Secretary of Defense, acting through the Under Secretary of Defense for Research and Engineering and in consultation with the Under Secretary of Defense for Acquisition and Sustainment, shall designate a single official or existing entity within the Department of Defense as the official or entity (as the case may be) with principal responsibility for guiding the direction of research and development of next generation software and software intensive systems for the Department, including the research and development of—

(1) new technologies for the creation of highly secure, reliable, and mission-critical software; and

(2) new approaches to software development, data-based analytics, and next generation management tools.

(b) DEVELOPMENT OF STRATEGY.—The official or entity designated under subsection (a) shall develop a Department-wide strategy for the research and development of next generation software and software intensive systems for the Department of Defense, including strategies for—

(1) types of software innovation efforts within the science and technology portfolio of the Department;

(2) investment in new approaches to software development, data-based analytics, and next generation management tools;

(3) ongoing research and other support of academic, commercial, and development community efforts to innovate the software development, engineering, and testing process;

(4) to the extent practicable, implementing the recommendations set forth in—

(A) the final report of the Defense Innovation Board submitted to the congressional defense committees under section 872 of the National Defense Authorization Act for Fiscal Year 2018 (Public Law 115–91; 131 Stat. 1497); and

(B) the final report of the Defense Science Board Task Force on the Design and Acquisition of Software for Defense Systems described in section 868 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Public Law 115–232; 10 U.S.C. 2223 note);

(5) supporting the acquisition, technology development, and test and operational needs of the Department through the development of capabilities, including personnel and infrastructure, and programs in—

(A) the science and technology reinvention laboratories (as designated under section 1105 of the National Defense Authorization Act for Fiscal Year 2010 (Public Law 111–84; 10 U.S.C. 2358 note));

(B) the facilities of the Major Range and Test Facility Base (as defined in section 2358a(f)(3) of title 10, United States Code); and

(C) the Defense Advanced Research Projects Agency; and

(6) the transition of relevant capabilities and technologies to information technology programs of the Department, including software intensive tactical systems, enterprise systems, and business systems.

(c) SUBMITTAL TO CONGRESS.—Not later than one year after the date of the enactment of this Act, the official or entity designated under subsection (a) shall submit to the congressional defense committees the strategy developed under subsection (b).

SEC. 2___[Log 69724]. MASTER PLAN FOR INFRASTRUCTURE REQUIRED TO SUPPORT RESEARCH, DEVELOPMENT, TEST, AND EVALUATION MISSIONS.

(a) PLAN REQUIRED.—The Secretary of Defense, in consultation with the Secretaries of the military departments, shall develop and implement a master plan that addresses the research, development, test, and evaluation infrastructure and modernization requirements of the Department of Defense, including the science and technology reinvention laboratories and the facilities of the Major Range and Test Facility Base.

(b) ELEMENTS.—The master plan required under subsection (a) shall include, with respect to the research, development, test, and evaluation infrastructure of the Department of Defense, the following:

(1) A summary of deficiencies in the infrastructure, by location, and the effect of the deficiencies on the ability of the Department—

(A) to meet current and future military requirements identified in the National Defense Strategy;

(B) to support science and technology development and acquisition programs; and

(C) to recruit and train qualified personnel.

(2) A summary of existing and emerging military research, development, test, and evaluation mission areas, by location, that require modernization investments in the infrastructure—

(A) to improve operations in a manner that may benefit all users;

(B) to enhance the overall capabilities of the research, development, test, and evaluation infrastructure, including facilities and resources;

(C) to improve safety for personnel and facilities; and

(D) to reduce the long-term cost of operation and maintenance.

(3) Identification of specific infrastructure projects that are required to address the infrastructure deficiencies identified under paragraph (1) or to support the existing and emerging mission areas identified under paragraph (2).

(4) For each project identified under paragraph (3)—

(A) a description of the scope of work;

(B) a cost estimate;

(C) a summary of the plan for the project;

(D) an explanation of the level of priority that will be given to the project; and

(E) a schedule of required infrastructure investments.

(5) A description of how the Department, including each military department concerned, will carry out the infrastructure projects identified in paragraph (3) using the range of authorities and methods available to the Department, including—

(A) military construction authority under section 2802 of title 10, United States Code;

(B) unspecified minor military construction authority under section 2805(a) of such title;

(C) laboratory revitalization authority under section 2805(d) of such title;

(D) the authority to carry out facility repair projects, including the conversion of existing facilities, under section 2811 of such title;

(E) the authority provided under the Defense Laboratory Modernization Pilot Program under section 2803 of the National Defense Authorization Act for Fiscal Year 2016 (Public Law 114–92; 10 U.S.C. 2358 note);

(F) methods that leverage funding from entities outside the Department, including public-private partnerships, enhanced use leases, real property exchanges; and

(G) any other authorities and methods determined to be appropriate by the Secretary of Defense.

(6) Identification of any statutory, regulatory, or policy barriers to implementing the master plan and regulatory, policy, or legislative proposals to address such barriers.

(c) CONSULTATION AND USE OF CONTRACT AUTHORITY.—In implementing the plan required under subsection (a), the Secretary of Defense shall—

(1) consult with existing and anticipated users of the Major Range and Test Facility Base; and

(2) consider using the contract authority provided to the Secretary under section 2681 of title 10, United States Code.

(d) SUBMISSION TO CONGRESS.—Not later than October 30, 2020, the Secretary of Defense shall submit to the congressional defense committees the master plan developed under subsection (a).

(e) RESEARCH AND DEVELOPMENT INFRASTRUCTURE DEFINED.—In this section, the term ''research, de-

velopment, test, and evaluation infrastructure'' means the infrastructure of—

(1) the science and technology reinvention laboratories (as designated under section 1105 of the National Defense Authorization Act for Fiscal Year 2010 (Public Law 111–84 ; 10 U.S.C. 2358 note));

(2) the Major Range and Test Facility Base (as defined in section 2358a(f)(3) of title 10, United States Code); and

(3) other facilities that support the research development, test, and evaluation activities of the Department.

SEC. 2___[Log 69845]. PROGRAM ON ENHANCEMENT OF PREPARATION OF DEPENDENTS OF MEMBERS OF ARMED FORCES FOR CAREERS IN SCIENCE, TECHNOLOGY, ENGINEERING, AND MATHEMATICS.

(a) PROGRAM REQUIRED.—Chapter 111 of title 10, United States Code, is amended by inserting after section 2192a the following new section:

"§ 2192b. Program on enhancement of preparation of dependents of members of armed forces for careers in science, technology, engineering, and mathematics

''(a) PROGRAM REQUIRED.—The Secretary of Defense shall carry out a program to—

''(1) enhance the preparation of students at covered schools for careers in science, technology, engineering, and mathematics; and

''(2) provide assistance to teachers at covered schools to enhance preparation described in paragraph (1).

''(b) COORDINATION.—In carrying out the program, the Secretary shall coordinate with the following:

''(1) The Secretaries of the military departments.

''(2) The Secretary of Education.

''(3) The National Science Foundation.

''(4) Other organizations as the Secretary of Defense considers appropriate.

''(c) ACTIVITIES.—Activities under the program may include the following:

''(1) Establishment of targeted internships and cooperative research opportunities at defense laboratories and other technical centers for students and teachers at covered schools.

''(2) Establishment of scholarships and fellowships for students at covered schools.

''(3) Efforts and activities that improve the quality of science, technology, engineering, and mathematics educational and training opportunities for students and teachers at covered schools, including with respect to improving the development of curricula at covered schools.

''(4) Development of travel opportunities, demonstrations, mentoring programs, and informal science education for students and teachers at covered schools.

''(d) METRICS.—The Secretary shall establish outcome-based metrics and internal and external assessments to evaluate the merits and benefits of activities conducted

under the program with respect to the needs of the Department of Defense.

''(e) COVERED SCHOOLS DEFINED.—In this section, the term 'covered schools' means elementary or secondary schools at which the Secretary determines a significant number of dependents of members of the armed forces are enrolled.''.

(b) CLERICAL AMENDMENT.—The table of sections at the beginning of such chapter is amended by inserting after the item relating to section 2192a the following new item:

''2192b. Program on enhancement of preparation of dependents of members of armed forces for careers in science, technology, engineering, and mathematics.''.

(c) CONFORMING REPEAL.—Section 233 of the Carl Levin and Howard P. ''Buck'' McKeon National Defense Authorization Act for Fiscal Year 2015 (Public Law 113–291; 10 U.S.C. 2193a note) is repealed.

SEC. 2___[Log 69236]. GRANTS FOR CIVICS EDUCATION PROGRAMS.

(a) IN GENERAL.—The Secretary of Defense shall carry out a program under which the Secretary makes grants to eligible entities, on a competitive basis, to support the development and evaluation of civics education programs.

(b) APPLICATION.—To be eligible to receive a grant under this section an eligible entity shall submit to the Secretary of Defense an application at such time, in such manner, and containing such information as the Secretary may require. Applications submitted under this subsection shall be evaluated on the basis of merit pursuant to competitive procedures prescribed by the Secretary of Defense.

(c) SELECTION CRITERIA.— To be selected to receive a grant under this section an eligible entity shall demonstrate each of the following to the satisfaction of the Secretary:

(1) The civics education program proposed by the entity will include innovative approaches for improving civics education.

(2) The entity will dedicate sufficient resources to the program.

(3) As part of the program, the entity will conduct evaluations in accordance with subsection (f)(1)(B).

(4) The entity will carry out activities to disseminate the results of the evaluations described in such subsection, including publication of the results in peer-reviewed academic journals.

(d) GEOGRAPHIC DISTRIBUTION.—To the extent practicable, the Secretary of Defense shall ensure an equitable geographic distribution of grants under this section.

(e) CONSULTATION.—In awarding grants under this section, the Secretary of Defense shall consult with the Secretary of Education.

(f) USES OF FUNDS.—

(1) REQUIRED USES OF FUNDS.—An eligible entity that receives a grant under this section shall use such grant—

(A) to establish a civics education program or to improve an existing civics education program;

(B) to evaluate the effect of the program on participants, including with respect to—

(i) critical thinking and media literacy;

(ii) voting and other forms of political and civic engagement;

(iii) interest in employment, and careers, in public service;

(iv) understanding of United States law, history, and government; and

(v) the ability of participants to collaborate and compromise with others to solve problems.

(2) ALLOWABLE USES OF FUNDS.—An eligible entity that receives a grant under this section may use such grant for—

(A) the development or modification of curricula relating to civics education;

(B) classroom activities, thesis projects, individual or team projects, internships, or community service activities relating to civics;

(C) collaboration with government entities, non-profit organizations, or consortia of such entities and organizations to provide participants with civics-related experiences;

(D) civics-related faculty development programs;

(E) recruitment of educators who are highly qualified in civics education to teach civics or

to assist with the development of curricula for civics education;

(F) presentation of seminars, workshops, and training for the development of skills associated with civic engagement;

(G) activities that enable participants to interact with government officials and entities;

(H) expansion of civics education programs and outreach for members of the Armed Forces, dependents and children of such members and employees of the Department of Defense; and

(I) opportunities for participants to obtain work experience in fields relating to civics.

(g) DEFINITIONS.—In this section:

(1) The term ''civics education program'' means an educational program that provides participants with—

(A) knowledge of law, government, and the rights of citizens; and

(B) skills that enable participants to responsibly participate in democracy.

(2) The term ''eligible entity'' means a Department of Defense domestic dependent elementary or

secondary school (as described in section 2164 of title 10, United States Code).

SEC. 2___[Log 70033]. STRATEGY AND IMPLEMENTATION PLAN FOR FIFTH GENERATION INFORMATION AND COMMUNICATIONS TECHNOLOGIES.

(a) IN GENERAL.—Not later than 270 days after the date of the enactment of this Act, the Secretary of Defense shall develop—

(1) a strategy for harnessing fifth generation (commonly known as ''5G'') information and communications technologies to enhance military capabilities, maintain a technological advantage on the battlefield, and accelerate the deployment of new commercial products and services enabled by 5G networks throughout the Department of Defense; and

(2) a plan for implementing the strategy developed under paragraph (1).

(b) ELEMENTS.—The strategy required under subsection (a) shall include the following elements:

(1) Adoption and use of secure fourth generation (commonly known as ''4G'') communications technologies and the transition to advanced and secure 5G communications technologies for military applications.

(2) Science, technology, research, and development efforts to facilitate the advancement and adoption of 5G technology and new uses of 5G systems, subsystems, and components, including—

(A) 5G testbeds for developing military applications; and

(B) spectrum sharing technologies and frameworks.

(3) Strengthening engagement and outreach with industry, academia, international partners, and other departments and agencies of the Federal Government on issues relating to 5G technology.

(4) Defense industrial base supply chain risk, management, and opportunities.

(5) Preserving the ability of the Joint Force to achieve objectives in a contested and congested spectrum environment.

(6) Strengthening the ability of the Joint Force to conduct full spectrum operations that enhance the military advantages of the United States.

(7) Securing the information technology and weapon systems of the Department against malicious activity.

(8) Such other matters as the Secretary of Defense determines to be relevant.

(c) CONSULTATION.—In developing the strategy and implementation plan required under subsection (a), the Secretary of Defense shall consult with the following:

(1) The Chief Information Officer of the Department of Defense.

(2) The Under Secretary of Defense for Research and Engineering.

(3) The Under Secretary of Defense for Acquisition and Sustainment.

(4) The Under Secretary of Defense for Intelligence.

(5) Service Acquisition Executives of each military service.

(d) BRIEFING.—Not later than 180 days after the date of the enactment of this Act, the Secretary of Defense shall provide to the congressional defense committees a briefing on the progress of the Secretary in developing the strategy and implementation plan required under subsection (a).

SEC. 2___[Log 70089]. ARTIFICIAL INTELLIGENCE EDUCATION STRATEGY.

(a) STRATEGY REQUIRED.—

(1) IN GENERAL.—The Secretary of Defense shall develop a strategy for educating service members in relevant occupational fields on matters relating to artificial intelligence.

(2) ELEMENTS.—The strategy developed under subsection (a) shall include a curriculum designed to give service members a basic knowledge of artificial intelligence. The curriculum shall include instruction in—

(A) artificial intelligence design;

(B) software coding;

(C) potential military applications for artificial intelligence;

(D) the impact of artificial intelligence on military strategy and doctrine;

(E) artificial intelligence decision making via machine learning and neural networks;

(F) ethical issues relating to artificial intelligence;

(G) the potential biases of artificial intelligence;

(H) potential weakness in artificial intelligence technology; and

(I) any other matters the Secretary of Defense determines to be relevant.

(b) IMPLEMENTATION PLAN.—

(1) IN GENERAL.—The Secretary of Defense shall develop a plan for implementing the strategy developed under subsection (a).

(2) ELEMENTS.—The implementation plan required under paragraph (1) shall identify the following:

(A) The military occupational specialties (applicable to enlisted members and officers) that are most likely to involve interaction with artificial intelligence technology.

(B) The specific occupational specialties that will receive training in accordance with the curriculum described in subsection (a)(2).

(C) The duration of the training.

(D) The context in which the training will be provided, which may include basic training, occupationally specific training, and professional military education.

(E) Metrics for evaluating the effectiveness of the training and curriculum.

(F) Any other issues the Secretary of Defense determines to be relevant.

(c) SUBMITTAL TO CONGRESS.—Not later than 270 days after the date of the enactment of this Act, the Secretary of Defense shall submit to the congressional defense committees—

(1) the strategy developed under subsection (a); and

(2) the implementation plan developed under subsection (b).

SEC. 8___.[Log 69857] EXTENSION OF SUNSET RELATING TO FEDERAL DATA CENTER CONSOLIDATION INITIATIVE.

Subsection (e) of section 834 of the National Defense Authorization Act for Fiscal Year 2015 (44 U.S.C. 3601 note) is amended by striking ''2020'' and inserting ''2022''.

SEC. 10___[Log 69195]. ANNUAL BUDGET JUSTIFICATION DISPLAY FOR SERVICE-COMMON AND OTHER SUPPORT AND ENABLING CAPABILITIES FOR SPECIAL OPERATIONS FORCES.

(a) IN GENERAL.—Chapter 9 of title 10, United States Code, is amended by inserting after section 225 the following new section:

"§ 226. Special operations forces: display of service-common and other support and enabling capabilities

''(a) IN GENERAL.—The Secretary shall include, in the budget materials submitted to Congress under section 1105 of title 31 for fiscal year 2021 and any subsequent fiscal year, a consolidated budget justification display showing service-common and other support and enabling capabilities for special operations forces requested by a military service or Defense Agency. Such budget justification display shall include any amount for service-common or other capability development and acquisition, training, operations, pay, base operations sustainment, and other common services and support.

''(b) SERVICE-COMMON AND OTHER SUPPORT AND ENABLING CAPABILITIES.—In this section, the term 'service-common and other support and enabling capabilities'

means capabilities provided in support of special operations that are not reflected in Major Force Program-11 or designated as special operations forces-peculiar.''.

(b) CLERICAL AMENDMENT.—The table of sections at the beginning of such chapter is amended by inserting after the item relating to section 225 the following new item:

''226. Special operations forces: display of service-common programs and activities.''.

SEC. 10___. [LOG 69217] NOTIFICATION ON THE PROVISION OF DEFENSE SENSITIVE SUPPORT.

Section 1055(b) of the National Defense Authorization Act for Fiscal Year 2017 (Public Law 114–328; 10 U.S.C. 113 note) is amended—

(1) in paragraph (2)—

(A) by redesignating subparagraph (C) as subparagraph (E); and

(B) by inserting after subparagraph (B) the following new subparagraphs:

''(C) A description of the required duration of the support.

''(D) A description of the initial costs for the support.''; and

(2) by adding at the end the following new paragraph:

''(5) SUSTAINMENT COSTS.—If the Secretary determines that sustainment costs will be incurred as a result of the provision of defense sensitive support, the Secretary, not later than 72 hours after the initial provision of such support, shall certify to the congressional defense committees (and the congressional intelligence committees with respect to matters relating to members of the intelligence com-

munity) that such sustainment costs will not interfere with the ability of the Department to execute operations, accomplish mission objectives, and maintain readiness.''.

SEC. 10___[Log 69763]. EXTENSION OF NATIONAL SECURITY COMMISSION ON ARTIFICIAL INTELLIGENCE.

Section 1051 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Public Law 115–232) is amended—

(1) in subsection (c)(1), by striking ''180 days'' and inserting ''360 days''; and

(2) in subsection (e), by striking ''October 1, 2020'' and inserting ''March 1, 2021''.

SEC. 10___[Log 69197]. ANNUAL REPORT ON JOINT MILITARY INFORMATION SUPPORT OPERATIONS WEB OPERATIONS CENTER.

(a) IN GENERAL.—Not later than March 1 of 2020, and each subsequent year until the termination date specified in subsection (c), the Commander of United States Special Operations Command shall submit to the congressional defense committees a report on the activities of the Joint Military Information Support Operations Web Operations Center (hereinafter referred to as the ''JMWC'') during the most recently concluded fiscal year.

(b) CONTENTS OF REPORT.—The report required by subsection (a) shall include each of the following, for the fiscal year covered by the report:

(1) Definitions of initial operating capability and full operational capability as such terms relate to the JMWC.

(2) A detailed description of all activities conducted towards achieving initial operating capability and full operational capability of the JMWC.

(3) A list of all associated funding requested for each program element for achieving initial operating capability and full operational capability.

(4) A detailed description of validated doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policy requirements relating to establishment of the JMWC.

(5) A description of current JMWC capabilities, including information technology infrastructure and contractual arrangements.

(6) A list of all physical locations hosting JMWC capabilities.

(7) The number of military, contractor, and civilian personnel associated with the JMWC and any affiliated agency, service, or other Department of Defense entity.

(8) A description of the JMWC personnel organizational structure.

(9) An identification of inherently governmental functions relating to administration of the JMWC and execution of Military Information Support Operations (hereinafter referred to as ''MISO)'' programs hosted by the JMWC.

(10) A detailed description of frameworks, metrics, and capabilities established to measure the effectiveness of MISO programs hosted by the JMWC.

(11) A list of all associated funding requested by program element from each of the geographic combatant commanders for MISO programs hosted by the JMWC and a description of such MISO activities.

(12) An assessment of the effectiveness of MISO programs hosted by the JMWC.

(13) A description of efforts and activities conducted to share best practices and leverage lessons learned across the Department of Defense relating to MISO programs hosted by the JMWC, as well as a description of such best practices and lessons learned.

(14) An identification of liaisons and detailees to the JMWC from agencies and elements of the Department of Defense.

(15) Activities and efforts conducted to synchronize and deconflict MISO programs within the Department of Defense and with interagency and international partners related to strategic communications, as appropriate.

(16) Such other information as the Commander determines appropriate.

(c) TERMINATION.—The requirement to submit a report under this section shall terminate on January 1, 2025.

SEC. 10___[Log 69198]. ASSESSMENT OF SPECIAL OPERATIONS FORCE STRUCTURE.

(a) ASSESSMENT.—

(1) IN GENERAL.—The Secretary of Defense shall enter into an agreement with a federally funded research and development center for the conduct of an independent assessment of the force structure and roles and responsibilities of special operations forces.

(2) SUBMISSION TO CONGRESS.—Not later than July 1, 2020 the Secretary shall submit to the congressional defense committees the results of the assessment required under paragraph (1).

(3) FORM.—The assessment required under paragraph (1) shall be submitted in unclassified form, but may contain a classified annex.

(b) MATTERS TO BE CONSIDERED.—In performing the assessment under this section, the federally funded research and development center shall consider the following matters:

(1) The most recent national defense strategy under section 113(g) of title 10, United States Code.

(2) Special operations activities, as described in section 167(k) of title 10, United States Code.

(3) Potential future national security threats to the United States.

(4) Ongoing counterterrorism and contingency operations of the United States.

(5) The demand for special operations forces by geographic combatant commanders for security cooperation, exercises, and other missions that could be executed by conventional forces.

(6) Other government and non-government analyses that would contribute to the assessment through variations in study assumptions or potential scenarios.

(7) The role of emerging technology on special operations forces.

(8) Opportunities for reduced operation and sustainment costs of special operations.

(9) Current and projected capabilities of other United States Armed Forces that could affect force structure capability and capacity requirements of special operations forces.

(10) The process by which United States Special Operations Command determines force size and structure.

(11) The readiness of special operations forces for assigned missions and future conflicts.

(12) The adequacy of special operations force structure for meeting the goals of the National Military Strategy under section 153(b) of title 10, United States Code.

(13) Any other matters deemed relevant.

(c) ASSESSMENT RESULTS.—The results of the assessment under this section shall include each of the following:

(1) Considerations and recommendations for improving the readiness of special operations forces and alternative force structure options.

(2) Legislative recommendations with respect to section 167 of title 10, United States Code, and other relevant provisions of law.

(3) The views of United States Special Operations Command on the assessment.

SEC. 10___[Log 69194]. PROCESSES AND PROCEDURES FOR NOTIFICATIONS REGARDING SPECIAL OPERATIONS FORCES.

(a) IN GENERAL.—Not later than 180 days after enactment of this Act, the Secretary of Defense shall establish and submit to the congressional defense committees processes and procedures for providing notifications to the committees regarding members of special operations forces, as identified in section 167(j) of title 10, United States Code.

(b) PROCESSES AND PROCEDURES.—The processes and procedures established under subsection (a) shall—

(1) clarify the roles and responsibilities of the Secretaries of the military departments, the Assistant Secretary of Defense for Special Operations and Low Intensity Conflict, and the Commander of United States Special Operations Command;

(2) provide guidance relating to the types of matters that would warrant congressional notification, including awards, reprimands, incidents, and any other matters the Secretary determines necessary;

(3) be consistent with the national security of the United States;

(4) be designed to protect sensitive information during an ongoing investigation;

(5) account for the privacy of members of the Armed Forces; and

(6) take in to account existing processes and procedures for notifications to the congressional defense committees regarding members of the conventional Armed Forces.

SEC. ___. [LOG 69196] EXTENSION AND MODIFICATION OF NATO SPECIAL OPERATIONS HEADQUARTERS.

(a) AUTHORIZATION.—Subsection (a) of section 1244 of the National Defense Authorization Act for Fiscal Year 2010 (Public Law 111–84; 123 Stat. 2541) is amended by striking ''2020'' and inserting ''2023''.

(b) REPEAL OF CERTIFICATION; LIMITATION.—Such section is amended—

(1) by striking subsection (c); and

(2) by inserting after subsection (b) the following new subsection:

''(c) LIMITATION.—Of the amounts made available under subsection (a) for fiscal year 2020, not more than 90 percent of such amounts may be obligated or expended until the Secretary of Defense, acting through the Assistant Secretary of Defense for Special Operations and Low Intensity Conflict, submits to the congressional defense committees a report on the rearrangement of responsibilities for overseeing and supporting NSHQ from U.S. Special Operations Command to U.S. European Command in 2019, including—

''(1) a justification and description of the impact of such rearrangement; and

''(2) a description of how such rearrangement will strengthen the role of the NSHQ in fostering special operations capabilities within NATO.''.

(c) ANNUAL REPORT.—Such section, as so amended, is further amended by adding at the end the following new subsection:

''(d) ANNUAL REPORT.—Not later than March 1 of each year until 2024, the Secretary of Defense shall submit to the congressional defense committees and the Committee on Foreign Relations of the Senate and the Committee on Foreign Affairs of the House of Representatives a report regarding support for the NSHQ. Each report shall include the following:

''(1) The total amount of funding provided by the United States and other NATO nations to the NSHQ for operating costs of the NSHQ.

''(2) A description of the activities carried out with such funding, including—

''(A) the amount of funding allocated for each such activity;

''(B) the extent to which other NATO nations participate in each such activity;

''(C) the extent to which each such activity is carried out in coordination or cooperation with the Joint Special Operations University;

''(D) the extent to which each such activity is carried out in relation to other security cooperation activities, exercises, or operations of the Department of Defense;

''(E) the extent to which each such activity is designed to meet the purposes set forth in paragraphs (1) through (5) of subsection (b); and

''(F) an assessment of the extent to which each such activity will promote the mission of the NSHQ.

''(3) Other contributions, financial or in kind, provided by the United States and other NATO nations in support of the NSHQ.

''(4) Any other matters that the Secretary of Defense considers appropriate.''.

SEC. 16___. [LOG 69272] SURVEY AND REPORT ON ALIGNMENT OF INTELLIGENCE COLLECTIONS CAPABILITIES AND ACTIVITIES WITH DEPARTMENT OF DEFENSE REQUIREMENTS.

(a) SURVEY AND REVIEW.—

(1) IN GENERAL.—Not later than 120 days after the date of the enactment of this Act, the Under Secretary of Defense for Intelligence, in coordination with the Chairman of the Joint Chiefs of Staff and the Director of National Intelligence, shall—

(A) review the organization, posture, current and planned investments, and processes of the intelligence collections capabilities and activities, for the purpose of assessing the sufficiency, integration, and interoperability of such capabilities and activities to support the current and future requirements of the Department of Defense; and

(B) conduct a survey of each geographic and functional combatant command, with respect to intelligence collections capabilities and activities, to assess—

(i) the current state of the support of such capabilities and activities to military operations;

(ii) whether the posture of such capabilities and activities is sufficient to address the requirements of the Department of Defense;

(iii) the extent to which such capabilities and activities address gaps and deficiencies with respect to the operational requirements of the Global Campaign Plans, as identified in the most recent readiness reviews conducted by the Joint Staff; and

(iv) whether current and planned investments in such capabilities and activities are sufficient to address near-, mid-, and long-term spaceborne, airborne, terrestrial, and human collection capability requirements.

(2) ELEMENTS.—The survey and review under paragraph (1) shall include the following:

(A) A comprehensive assessment of intelligence collections capabilities and activities, and whether such capabilities and activities—

(i) are appropriately postured and sufficiently resourced to meet current and future requirements of the Department of Defense;

(ii) are appropriately balanced to address operational and strategic defense intelligence requirements; and

(iii) are sufficiently integrated and interoperable between activities of the Military Intelligence Program and the National Intelligence Program to respond to emerging requirements of the Department of Defense.

(B) With respect to each geographic and functional combatant command—

(i) information on the gaps and deficiencies, by specific intelligence capability type, described in paragraph (1)(B)(iii);

(ii) a review of the alignment of such gaps and deficiencies with the intelligence, surveillance, and reconnaissance submissions to the integrated priorities list for the period beginning with the completion of the most recent readiness reviews conducted by the Joint Staff and ending on

the date of the commencement of the survey and review under subsection (a); and

(iii) detailed information on the allocation and realignment of intelligence collections capabilities and activities to address—

(I) such gaps and deficiencies; and

(II) such intelligence, surveillance, and reconnaissance submissions.

(b) REPORT.—

(1) SUBMISSION.—Not later than 270 days after the date of the enactment of this Act, the Under Secretary of Defense for Intelligence shall submit to the appropriate congressional committees a report on the findings of the Under Secretary with respect to the survey and review under subsection (a)(1).

(2) CONTENT.—The report under paragraph (1) shall include—

(A) an evaluation of—

(i) the organization, posture, current and planned investments, and processes of the intelligence collections capabilities and

activities, including the extent to which such capabilities and activities enable the geographic and functional combatant commands to meet the operational and strategic requirements of the Department of Defense;

(ii) the use or planned use by each geographic and functional combatant command of intelligence collections capabilities and activities available to such command to address operational and strategic requirements of the Department of Defense;

(iii) the gaps and deficiencies described in (a)(1)(B)(iii), if any, that prohibit each geographic and functional combatant command from the most effective use of the intelligence collections capabilities and activities to address priority requirements of the Department of Defense;

(iv) the accepted risk by the Secretary of Defense from the prioritization of certain Department of Defense requirements with respect to the allocation of intelligence collections capabilities and activities; and

(v) the alignment and responsiveness of intelligence collections capabilities and activities with respect to the planning requirements for the Program of Analysis of each combat support agency that is part of—

(I) the Defense Intelligence Enterprise; and

(II) the intelligence community; and

(B) recommendations, if any, to improve the sufficiency, responsiveness, and interoperability of intelligence collections capabilities and activities to fulfill the operational and strategic requirements of the Department of Defense.

(3) FORM.—The report under paragraph (1) shall be submitted in unclassified form without any designation relating to dissemination control, but may contain a classified annex.

(c) DEFINITIONS.—In this section:

(1) The term ''appropriate congressional committees'' means—

(A) the congressional defense committees; and

(B) the congressional intelligence committees.

(2) The term ''combat support agency'' has the meaning given that term in section 193(f) of title 10, United States Code.

(3) The term ''Defense Intelligence Enterprise'' has the meaning given that term in section 1633(c)(2) of the National Defense Authorization Act for Fiscal Year 2017 (Public Law 114–328; 130 Stat. 2600).

(4) The term ''intelligence collections capabilities and activities'' means the totality of intelligence collections systems and processes which enable the tasking, processing, exploitation, and dissemination capabilities, capacity, and activities of the Defense Intelligence Enterprise.

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

(6) The term ''congressional intelligence committees'' has the meaning given that term in section 3 of the National Security Act of 1947 (50 U.S.C. 3003).

SEC. 16___. [LOG 69292] MODIFICATIONS TO ISR INTEGRATION COUNCIL AND ANNUAL BRIEFING REQUIREMENTS.

(a) ISR INTEGRATION COUNCIL.—Subsection (a) of section 426 of title 10, United States Code, is amended to read as follows:

''(a) ISR INTEGRATION COUNCIL.—(1) The Under Secretary of Defense for Intelligence shall establish an Intelligence, Surveillance, and Reconnaissance Integration Council—

''(A) to assist the Secretary of Defense in carrying out the responsibilities of the Secretary under section 105(a) of the National Security Act of 1947 (50 U.S.C. 3038(a));

''(B) to assist the Under Secretary with respect to matters relating to—

''(i) integration of intelligence and counterintelligence capabilities and activities under section 137(b) of this title of the military departments, intelligence agencies of the Department of Defense, and relevant combatant commands; and

''(ii) coordination of related developmental activities of such departments, agencies, and combatant commands; and

''(C) to otherwise provide a means to facilitate such integration and coordination.

''(2) The Council shall be composed of—

''(A) the Under Secretary, who shall chair the Council;

''(B) the directors of the intelligence agencies of the Department of Defense;

''(C) the senior intelligence officers of the armed forces and the regional and functional combatant commands;

''(D) the Director for Intelligence of the Joint Chiefs of Staff; and

''(E) the Director for Operations of the Joint Chiefs of Staff.

''(3) The Under Secretary shall invite the participation of the Director of National Intelligence (or a representative of the Director) in the proceedings of the Council.

''(4) The Under Secretary may designate additional participants to attend the proceedings of the Council, as the Under Secretary determines appropriate.''.

(b) ANNUAL BRIEFINGS.—Such section is further amended by striking subsections (b) and (c) and inserting the following new subsection (b):

''(b) ANNUAL BRIEFINGS ON THE INTELLIGENCE AND COUNTERINTELLIGENCE REQUIREMENTS OF THE COMBATANT COMMANDS.—(1) The Chairman of the Joint Chiefs of Staff shall provide to the congressional defense committees and the congressional intelligence committees a briefing on the following:

''(A) The intelligence and counterintelligence requirements, by specific intelligence capability type, of each of the relevant combatant commands.

''(B) For the year preceding the year in which the briefing is provided, the fulfillment rate for each of the relevant combatant commands of the validated intelligence and counterintelligence requirements, by specific intelligence capability type, of such combatant command.

''(C) A risk analysis identifying the critical gaps and shortfalls in efforts to address operational and strategic requirements of the Department of Defense that would result from the failure to fulfill the validated intelligence and counterintelligence requirements of the relevant combatant commands.

"(D) A mitigation plan to balance and offset the gaps and shortfalls identified under subparagraph (C), including with respect to spaceborne, airborne, ground, maritime, and cyber intelligence, surveillance, and reconnaissance capabilities.

"(E) For the year preceding the year in which the briefing is provided—

"(i) the number of intelligence and counterintelligence requests of each commander of a relevant combatant command determined by the Joint Chiefs of Staff to be a validated requirement, and the total of capacity of such requests provided to each such commander;

"(ii) with respect to such validated requirements—

"(I) the quantity of intelligence and counterintelligence capabilities or activities, by specific intelligence capability type, that the Joint Chiefs of Staff requested each military department to provide; and

"(II) the total of capacity of such requests so provided by each such military department; and

"(iii) a qualitative assessment of the alignment of intelligence and counterintelligence ca-

pabilities and activities with the program of analysis for each combat support agency and intelligence center of a military service that is part of—

''(I) the Defense Intelligence Enterprise; and

''(II) the intelligence community.

''(2) The Under Secretary of Defense for Intelligence shall provide to the congressional defense committees and the congressional intelligence committees a briefing on short-, mid-, and long-term strategies to address the validated intelligence and counterintelligence requirements of the relevant combatant commands, including with respect to spaceborne, airborne, ground, maritime, and cyber intelligence, surveillance, and reconnaissance capabilities.

''(3) The briefings required by paragraphs (1) and (2) shall be provided at the same time that the President's budget is submitted pursuant to section 1105(a) of title 31 for each of fiscal years 2021 through 2025.

''(4) In this subsection:

''(A) The term 'congressional intelligence committees' has the meaning given that term in section 3 of the National Security Act of 1947 (50 U.S.C. 3003).

''(B) The term 'Defense Intelligence Enterprise' means the organizations, infrastructure, and measures, including policies, processes, procedures, and products, of the intelligence, counterintelligence, and security components of each of the following:

''(i) The Department of Defense.

''(ii) The Joint Staff.

''(iii) The combatant commands.

''(iv) The military departments.

''(v) Other elements of the Department of Defense that perform national intelligence, defense intelligence, intelligence-related, counterintelligence, or security functions.

''(C) The term 'fulfillment rate' means the percentage of combatant command intelligence and counterintelligence requirements satisfied by available, acquired, or realigned intelligence and counterintelligence capabilities or activities.

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

SEC. 16___.[LOG69212] NOTIFICATION REQUIREMENTS FOR SENSITIVE MILITARY CYBER OPERATIONS.

Section 395 of title 10, United States Code, is amended—

(1) in subsection (b)(3), by inserting ", signed by the Secretary," after "written notification"; and

(2) in subsection (c)—

(A) in paragraph (1)—

(i) in subparagraph (A), by striking "and" after the semicolon at the end;

(ii) by redesignating subparagraph (B) as subparagraph (C); and

(iii) by inserting after subparagraph (A) the following new subparagraph:

"(B) is determined to—

"(i) have a medium or high collateral effects estimate;

"(ii) have a medium or high intelligence gain or loss;

"(iii) have a medium or high probability of political retaliation, as determined by the political military assessment contained within the associated concept of operations;

''(iv) have a medium or high probability of detection when detection is not intended; or

''(v) result in medium or high collateral effects; and''; and

(B) in paragraph (2)(B), by striking ''outside the Department of Defense Information Networks to defeat an ongoing or imminent threat''.

SEC. 16___.[Log69213] TIER 1 EXERCISE OF SUPPORT TO CIVIL AUTHORITIES FOR A CYBER INCIDENT.

Section 1648 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 is amended—

(1) in subsection (a), by striking ''The'' and inserting ''Not later than February 1, 2020, the''; and

(2) by adding at the end the following new subsection:

''(c) LIMITATION.—Of the funds authorized to be appropriated by this Act or otherwise made available for fiscal year 2020 for the Department of Defense for the White House Communications Agency, not more than 90 percent of such funds may be obligated or expended until the initiation of the tier 1 exercise required under subsection (a).''.

SEC. 16___.[Log69214] EXTENSION OF THE CYBERSPACE SOLARIUM COMMISSION.

Paragraph (1) of section 1652(k) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Public Law 115–232) is amended by striking ''2019'' and inserting ''2020''.

SEC. 16___.[Log69216] NOTIFICATION OF DELEGATION OF AUTHORITIES TO THE SECRETARY OF DEFENSE FOR MILITARY OPERATIONS IN CYBERSPACE.

(a) IN GENERAL.—The Secretary of Defense shall provide written notification to the Committee on Armed Services of the House of Representatives and the Committee on Armed Services of the Senate of authorities delegated to the Secretary by the President for military operations in cyberspace that are otherwise held by the National Command Authority, not later than 15 days after any such delegation. Such notification shall include the following:

(1) A description of the authorities delegated to the Secretary.

(2) A description of relevant documents, including execute orders, issued by the Secretary in accordance with such authorities.

(3) A list of countries in which such authorities may be utilized.

(4) A description of authorized activities to be conducted or planned to be conducted pursuant to such authorities.

(5) Defined military objectives relating to such authorities.

(b) PROCEDURES.—

(1) IN GENERAL.—The Secretary of Defense shall establish and submit to the Committee on Armed Services of the House of Representatives and the Committee on Armed Services of the Senate procedures for complying with the requirements of subsection (a), consistent with the national security of the United States and the protection of operational integrity. The Secretary shall promptly notify the Committee on Armed Services of the House of Representatives and the Committee on Armed Services of the Senate in writing of any changes to such procedures at least 14 days prior to the adoption of any such changes.

(2) SUFFICIENCY.—The Committee on Armed Services of the House of Representatives and the Committee on Armed Services of the Senate shall ensure that committee procedures designed to protect from unauthorized disclosure classified information relating to national security of the United States are sufficient to protect the information that is submitted to the committees pursuant to this section.

(3) NOTIFICATION IN EVENT OF UNAUTHORIZED DISCLOSURE.—In the event of an unauthorized disclosure of authorities covered by this section, the Secretary of Defense shall ensure, to the maximum extent practicable, that the Committee on Armed Services of the House of Representatives and the Committee on Armed Services of the Senate are notified immediately. Notification under this paragraph may be verbal or written, but in the event of a verbal notification, a written notification signed by the Secretary shall be provided by not later than 48 hours after the provision of such verbal notification.

SEC. 16___.[log 69237] ANNUAL MILITARY CYBERSPACE OPERATIONS REPORT.

(a) IN GENERAL.—Not later than March 1 of each year, the Secretary of Defense shall provide to the congressional defense committees a written report detailing all military cyberspace operations conducted in the previous calendar year. For each such operation each such report shall include the following:

(1) An identification of the objective and purpose.

(2) Impacted information technology infrastructure, by location.

(3) A description of tools and capabilities utilized.

(4) An identification of the Cyber Mission Force team, or other Department of Defense entity or unit, that conducted such operation, and supporting teams, entities, or units.

(5) A description of the infrastructure and platforms on which such operation occurred.

(6) A description of relevant legal, operational, and funding authorities, including Execute Orders and Deployment Orders.

(7) Information relating to the total amount of funding required and associated program elements.

(8) Any other matters the Secretary determines relevant.

(b) CLASSIFICATION.—The Secretary of Defense shall provide each report required under subsection (a) at a classification level the Secretary determines appropriate.

(c) LIMITATION.—This section does not apply to cyber-enabled military information support operations.

(d) DEFINITION.—In this section, the term ''military cyberspace operations'' means defensive and offensive—

(1) cyber effects enabling operations, activities, and missions; and

(2) cyber effects operations, activities, and missions.

SEC. 16___.[Log69262] REPORT ON SYNCHRONIZATION OF EFFORTS RELATING TO CYBERSECURITY IN THE DEFENSE INDUSTRIAL BASE.

(a) REPORT.—Not later than May 1, 2020, the Secretary of Defense shall submit to the congressional defense committees a report on efforts, and roles and responsibilities, relating to cybersecurity in the Defense Industrial Base.

(b) ELEMENTS.—The report under subsection (a) shall include the following:

(1) Definitions for ''Controlled Unclassified Information'' (CUI) and ''For Official Use Only'' (FOUO), as well as policies regarding protecting information designated as such.

(2) A comprehensive list of Department of Defense programs to assist the Defense Industrial Base with cybersecurity compliance requirements of the Department.

(3) An evaluation of the resources and utilization of Department programs to assist the Defense Industrial Base in complying with cybersecurity compliance requirements referred to in paragraph (2).

(4) Optimal levels of resourcing required for activities, programs, and other Department efforts to assess and monitor compliance by the Defense Industrial Base with such cybersecurity compliance requirements.

(5) Roles and responsibilities of the Under Secretary of Defense for Acquisition and Sustainment, the Chief Information Officer, the Chief Management Officer, the Director of the Protecting Critical Technologies Task Force, and the Secretaries of the military services relating to the following:

(A) Establishing and ensuring compliance with cybersecurity standards, regulations, and policies.

(B) Deconflicting existing cybersecurity standards, regulations, and policies.

(C) Coordinating with and providing assistance to the Defense Industrial Base for cybersecurity matters, particularly such relates to the issues described in paragraphs (2), (3), and (8).

(6) Efforts to enhance the Department's visibility into its entire supply chain without violating privity.

(7) An evaluation of methodologies to tier cybersecurity requirements for the Defense Industrial Base relative to risk.

(8) Efforts to support and enhance threat information sharing between the Department and the Defense Industrial Base.

(9) An evaluation of a single Sector Coordinating Council for the Defense Industrial Base.

(10) An explanation of the Department's Protecting Critical Technologies Task Force efforts, and how its work will be incorporated into existing Department efforts.

(11) Any other information the Secretary of Defense determines relevant.

(c) DEFINITION.—In this section, the term ''Defense Industrial Base'' includes traditional and non-traditional defense contractors and academic institutions with contractual relationships with the Department of Defense related to activities involving information or technology requiring cybersecurity compliance.

SEC. 16___.[Log69562] EVALUATION OF CYBER VULNERABILITIES OF MAJOR WEAPON SYSTEMS OF THE DEPARTMENT OF DEFENSE.

Section 1647 of the National Defense Authorization Act for Fiscal Year 2016 is amended by adding at the end the following new subsections:

''(f) WRITTEN NOTIFICATION.—If the Secretary determines that the Department will not complete an evaluation of the cyber vulnerabilities of each major weapon system of the Department by the date specified in subsection (a)(1), the Secretary shall provide to the congressional defense committee written notification relating to each such incomplete evaluation. Such a written notification shall include the following:

''(1) An identification of each major weapon system requiring such an evaluation and the anticipated date of completion.

''(2) A justification for the inability to complete such an evaluation by the date specified in subsection (a)(1).

''(g) REPORT.—The Secretary, acting through the Assistant Secretary of Defense for Acquisition and Sustainment, shall provide a report to the congressional defense committees upon completion of the requirement

for an evaluation of the cyber vulnerabilities of each major weapon system of the Department under this section. Such report shall include the following:

''(1) An identification of cyber vulnerabilities of each major weapon system requiring mitigation.

''(2) An identification of current and planned efforts to address the cyber vulnerabilities of each major weapon system requiring mitigation, including efforts across the doctrine, organization, training, materiel, leadership and education, personnel, and facilities of the Department.

''(3) A description of joint and common cyber vulnerability mitigation solutions and efforts, including solutions and efforts across the doctrine, organization, training, materiel, leadership and education, personnel, and facilities of the Department.

''(4) A description of lessons learned and best practices regarding evaluations of the cyber vulnerabilities and cyber vulnerability mitigation efforts relating to major weapon systems.

''(5) A description of efforts to share lessons learned and best practices regarding evaluations of the cyber vulnerabilities and cyber vulnerability mitigation efforts of major weapon systems across the Department.

''(6) An identification of measures taken to institutionalize evaluations of cyber vulnerabilities of major weapon systems.

''(7) Information relating to guidance, processes, procedures, or other activities established to mitigate or address the likelihood of cyber vulnerabilities of major weapon systems by incorporation of lessons learned in the research, development, test, evaluation, and acquisition cycle, including promotion of cyber education of the acquisition workforce.

''(8) Any other matters the Secretary determines relevant.''.

SEC. 16___.[Log69612] BRIEFINGS ON THE STATUS OF THE NATIONAL SECURITY AGENCY AND UNITED STATES CYBER COMMAND PARTNERSHIP.

(a) IN GENERAL.—Not later than 90 days after the date of the enactment of this Act and quarterly thereafter, the Secretary of Defense and the Director of National Intelligence shall provide to the congressional defense committees and the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate briefings on the nature of the National Security Agency and United States Cyber Command's current and future partnership. Briefings under this section shall terminate on January 1, 2022.

(b) ELEMENTS.—Each briefing under this section shall include the following:

(1) Status updates on the current and future National Security Agency-United States Cyber Command partnership efforts.

(2) Executed documents, written memoranda of agreements or understandings, and policies issued governing such current and future partnership.

(3) Projected long term efforts.

(4) Updates related to the assessment required under section 1642 of the National Defense Authorization Act for Fiscal Year 2017 (relating to limitation on termination of dual-hat arrangement for Commander of the United States Cyber Command; Public Law 114–328).

SEC. 16___.[Log69622] LIMITATION OF FUNDING FOR CONSOLIDATED AFLOAT NETWORKS AND ENTERPRISE SERVICES.

Of the funds authorized to be appropriated by this Act or otherwise made available for fiscal year 2020 for the Consolidated Afloat Networks and Enterprise Services, not more than 85 percent of such funds may be obligated or expended until the Secretary of Defense, in coordination with the Chief Information Officer of the Department of Defense, certifies to the congressional defense committees that the recommendations in the Audit of Consolidated Afloat Networks and Enterprise Services Security Safeguards (DODIG-2019-072) have been implemented.

SEC. 16___.[Log69948] QUARTERLY CYBER OPERATIONS BRIEFINGS.

Subsection (b) of section 484 of title 10, United States Code, is amended—

(1) by redesignating paragraph (4) as paragraph (5); and

(2) by inserting after paragraph (3) the following new paragraph:

''(4) An overview of the readiness of the Cyber Mission Force to perform assigned missions.''.

DIRECTIVE REPORT LANGUAGE

Table Of Contents

Tactical Exploitation of National Capabilities Program
Transitioning the Function of Background Investigations to the Department of Defense
Unified Air Force Airborne Signals Intelligence Enterprise

DIVISION A—DEPARTMENT OF DEFENSE AUTHORIZATIONS

TITLE II—RESEARCH, DEVELOPMENT, TEST, AND EVALUATION

RESEARCH, DEVELOPMENT, TEST, AND EVALUATION, ARMY

Items of Special Interest

Army unfunded requirement for munitions storage

The committee recognizes the important work the Armaments Center, a science and technology reinvention laboratory at Picatinny Arsenal, plays in the ammunition life cycle to ensure our warfighters are appropriately equipped to complete their missions. The committee notes that the Under Secretary of Defense for Research and Engineering's February 2019 Report to Congress on Unfunded Requirements for Laboratory Military Construction Projects included for this center an unfunded laboratory minor science and technology military construction project for an Igloo Storage Installation. The committee directs the Secretary of the Army to provide a briefing to the House Committee on Armed Services not later than November 30, 2019, on what the Army's plans are to ensure that the required construction and maintenance is implemented to support this mission.

RESEARCH, DEVELOPMENT, TEST, AND EVALUATION, NAVY

Items of Special Interest

Advanced radar research

The committee notes there have been major advances in the field of radar development with respect to phased array radar technology in a digital design. The development of this technology is a critical enabler for the Navy in the development of tools to increase target detection as well as improve electronic warfare and adaptive sensing capabilities. The committee directs the Chief of Naval Research to submit a report to the House Committee on Armed Services not later than April 30, 2020, on its support of partnerships with laboratory-based antenna test facilities that help the Navy understand, characterize, and calibrate advanced all-digital radars that are under development.

High Energy Laser system integration

The committee is encouraged by the Navy's rapid demonstration of Laser Weapon Systems (LaWSs) on surface ships. In a short period of time, the Navy has deployed the 30 kilowatts (kW) LaWS on the USS Ponce (Afloat Forward Staging Base(Interim)-15) followed by the 150 kW Laser Weapon System Demonstrator

(LWSD) on the USS Portland (Landing Platform/Dock-27) in 2019. The improvements in power and beam quality make this a near 100 fold improvement in lethality. The committee is also encouraged by the 60 kW HELIOS program for integration on Destroyer Designated Guided ships by 2020. However, there appears to be more opportunity to integrate High Energy Laser (HEL) systems on large capital ships including aircraft carrier, fixed wing, nuclear powered (CVNs) and large amphibious ships to increase defensive capability and lethality of our expeditionary forces as evidenced by the deployment of LWSD on the USS Portland. The committee directs the Secretary of the Navy to submit a report to the congressional defense committees not later than April 1, 2020, describing a path forward for integration of HEL Systems 150-300 kW on large capital warships, including CVNs and large amphibious ships.

RESEARCH, DEVELOPMENT, TEST, AND EVALUATION, AIR FORCE

Items of Special Interest

Low-cost attritable aircraft technology

The committee supports the intent of the Assistant Secretary of the Air Force for Acquisition, Technology, and Logistics to accelerate the Air Force Research Laboratory's Low-Cost Attritable Aircraft Technology (LCAAT) program for collaborative pairing with manned platforms, potentially including the F–35. The committee views the combined application of commercial technology, autonomy, and artificial intelligence as imperative for solving current military challenges. Teams of low-cost collaborative systems provide new mechanisms to ensure survivability and mission success without leveraging exquisite technology and the associated high cost and long development timelines.

Integration and technology demonstrations reduce the risk and time required to transition technologies into operational systems. Accordingly, further prototyping and technology enhancements are necessary to transition the LCAAT demonstrator aircraft system into a fully operational capability. Continued testing and the development and integration of technology is required to provide a runway takeoff capability; airborne weapons deployment capability (in support of manned platforms); human machine interface enhancements; development and integration of a secure Common Data Link-based network system; and development of operations and maintenance systems, processes, and tests to operationalize the evolving Manned-Unmanned Teaming capability.

Accordingly, the committee directs the Assistant Secretary of the Air Force for Acquisition, Technology, and Logistics to submit a report to the House Committee on Armed Services not later than April 1, 2020, on the Air Force's efforts for the design, test, and integration of these air vehicles.

Unmanned aerial systems cyber operations research

The committee recognizes the critical importance of developing new technologies to detect and counter adversarial unmanned aerial systems (UAS) and UAS swarms. The committee notes that countering UAS operations presents a special series of unmet communications, command and control, cyber, computation, and intelligence challenges at the tactical edge. Due to this emerging threat, the committee directs the Director of the Air Force Research Laboratory Information Directorate to provide a briefing to the House Committee on Armed Services by October 30, 2019, on their continued research and development into the countering of unmanned aerial systems using advanced technologies to facilitate UAS detection and geolocation, determination of individual and swarm behavior, dissection of swarms to identify critical nodes, situational awareness, elucidation of threats and mission intent, and counter UAS capabilities.

RESEARCH, DEVELOPMENT, TEST, AND EVALUATION, DEFENSE-WIDE

Items of Special Interest

Additive manufacturing

Defense-wide Manufacturing Science and Technology (DMS&T) is the joint, defense-wide component of the Department of Defense's Manufacturing Technology (ManTech) program directed by section 2521 of title 10, United States Code. Investments in ManTech provide for a healthy industrial base necessary for national security. The committee is aware that eight Department Manufacturing Innovative Institutes are funded under DMS&T, including an institute focused on additive manufacturing. The committee believes that additive manufacturing supports improved life-cycle maintenance and readiness, especially when capabilities are provided in-theater. Therefore, the committee directs the Under Secretary of Defense for Research and Engineering to provide a briefing to the House Committee on Armed Services not later than October 1, 2019, on the DMS&T program investments in additive manufacturing and the value and efficiencies such investments may have, especially when capabilities are provided in-theater.

Analysis of Science and Technology Reinvention Laboratories

The committee recognizes that the Department of Defense's organic science and technology (S&T), research, development, and test ecosystem, to include the test centers and laboratories, struggles to compete with the tech sector in attracting and maintaining a talented workforce. These entities also face challenges in obtaining resources for military construction projects and other improvements as the Department has not prioritized investment in organic institutions. In fact, the Defense Science Board reported in 2017 that most Department laboratory directors feel they are unable to maintain their facilities and infrastructure at a reasonable standard.

The committee believes that the Department's in-house ecosystem is vital to maintaining a technological advantage for our warfighters, sustaining a healthy industrial base, and protecting the research and development of critical technologies. Many prior years' National Defense Authorization Acts have granted the Directors of the Science and Technology Reinvention Laboratories (STRLs) authorities to promote modernization and allow for hiring of technical talent. The committee understands most of these authorities have not been fully implemented by the Department and elsewhere in this Act, the committee includes two legislative provisions that would require the Secretary of Defense to establish plans for implementation.

The committee believes that comprehensive data and analysis relating to the STRLs available to senior leaders will promote better decision making and resource allocation to ensure these entities remain viable. Therefore, the committee directs the Director of Cost Assessment and Program Evaluation to conduct an independent analysis of the Department's STRL infrastructure, modernization, and workforce. The analysis shall include the components that comprise total costs at each facility; accounting practices with regards to direct and indirect costs as compared to other typical S&T entities; effects of labor cost-rate growth; the use of research and development funding for military construction projects; the loss of buying power on spending for materials, equipment and other non-labor resources; and any other matters deemed appropriate by the Director to maintain high-quality institutions. The Under Secretary of Defense for Research and Engineering shall provide the Director with the information and resources necessary. The Director shall provide the analysis to the House Committee on Armed Services by September 1, 2021.

Directed energy test range workloads

The committee remains concerned that U.S. Major Range and Test Facility Bases (MRTFBs) have inadequate infrastructure to support next generation weapon systems. The committee also recognizes the need to transition new and game-changing directed energy technologies to the warfighter. The Department of Defense established the Nation's first High Energy Laser System Test Facility (HELSTF) in 1975, but the technology has seen significant advancements over the course of four decades. As directed energy weapon systems mature, the need to validate their performance becomes increasingly important. The workload and number of directed energy demonstrations and exercises have increased significantly since 1975 and the projected workload for fiscal years 2018–22 for HELSTF is large and growing, and has expanded to include High Power Microwave (HPM) testing. Additionally, there are currently no available enduring frequency agile and tunable HPM assets for evolving doctrine or HPM Directed Energy Concept of Operations development any at MRTFBs.

The committee directs the Assistant Director for Directed Energy in the Office of the Under Secretary of Defense for Research and Engineering to provide a

briefing to the House Committee on Armed Services not later than September 30, 2019, on the test and evaluation infrastructure and test asset needs to meet directed energy requirements over the next 5 years. Included in this briefing should be the plans for HELSTF and other service MRTFB test sites, to include HPM testing, required for directed energy experimentation in order to develop the tactics, techniques, and procedures required to incorporate the emerging capabilities into the Department's inventory. This presentation should also include mitigation procedures for operations in the national aerospace system against above-the-horizon targets.

Electronic warfare planning for near-peer adversaries

The Department of Defense's 2013 Electromagnetic Spectrum Strategy recognizes that Department operations in all domains are fundamentally dependent on our use and control of the electromagnetic spectrum. All joint functions such as movement and maneuver, fires, command and control, intelligence, protection, sustainment, and information are accomplished with systems that use the spectrum. The safety and security of U.S. citizens, the effectiveness of U.S. combat forces, and the lives of U.S. military members, our allies, and non-combatants depend on spectrum access. More recently, in December 2018, the Government Accountability Office issued an Emerging Threats report that similarly echoed that adversaries are developing electronic attack weapons to target U.S. systems with sensitive electronic components, such as military sensors, communication, navigation, and information systems. These weapons are intended to degrade U.S. capabilities and could restrict situational awareness or may affect military operations. The committee is concerned about the extent to which the Department is planning and preparing to defend itself and operate in an environment where peer and near-peer adversaries could use existing and emerging capabilities that degrade use of the electromagnetic spectrum.

Therefore, the committee directs the Comptroller General of the United States to assess the Department's electronic warfare and electromagnetic spectrum operations strategy and implementation efforts. The assessment should include the current electronic warfare threat from peer or near-peer adversaries and actions the Department has taken in response to include the protection of critical warfighting capabilities; the extent to which the Department has incorporated current and emerging electromagnetic spectrum risks into service and combatant command operational planning efforts and exercises; the status and effectiveness of the Electronic Warfare Executive Committee established by the Secretary of Defense in 2015; the Department's implementation of the 2013 Electromagnetic Spectrum Strategy; and any other matters the Comptroller General determines to be relevant.

The committee further directs the Comptroller General to provide a briefing to the House Committee on Armed Services not later than March 1, 2020, on preliminary findings, and to present final results in a format and timeframe agreed to at the time of the briefing.

Human simulation and human factors modeling

Section 227 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Public Law 115-232) required the Secretary of Defense to develop and provide for the carrying out of human factors modeling and simulation activities with the purpose of accelerating research and development to enhance capabilities for human performance, human-systems integration, and training for the warfighter. The committee directs the Secretary of Defense to provide a briefing to the House Committee on Armed Services not later than January 30, 2020, on the status of this requirement. Specifically, the committee would like to know the extent of the activities implemented, the effects as yet of these activities with respect to their purpose, which activity participants, locations of the activities, and the plan to sustain these activities going forward.

Hypersonic test infrastructure and workforce

The committee acknowledges the joint-effort to expand and develop conventional prompt strike capabilities (CPS), which was codified in a memorandum of agreement between the Department of Defense, military services, and the Missile Defense Agency to deliver hypersonic boost glide technology. To achieve success in the multiple service efforts to deliver CPS capabilities, the committee recognizes the importance of state-of-the-art facilities and infrastructure to support research, development, prototyping, testing, and deployment.

The committee notes that recent advances have been made in high temperature manufacturing, hypersonic wind tunnel capability and material testing technology. Specifically, the committee is encouraged by the Department's efforts to expand the number of hypersonic wind tunnel and testing facilities, specifically at Arnold Air Force Base Engineering Development Center and the joint-investment at several universities, including Purdue, Notre Dame, and Texas A&M. However, even with these increases, current facilities will be stressed to provide the level of testing needed across the joint-efforts.

In addition to the high demand for testing infrastructure, the U.S. currently lacks the workforce with sufficient knowledge and experience in hypersonic materials manufacturing and testing to develop these next generation systems. Therefore, the committee directs the Under Secretary of Defense for Research and Engineering, in coordination with the military services and Missile Defense Agency, to provide a report to the House Committee on Armed Services not later than December 31, 2019, on the health of hypersonic testing technologies and workforce. The report should include an analysis of current capacity to meet existing requirements, options to improve testing facilities, with cost, schedule, and operational considerations, and efforts that are being taken to address workforce gaps.

The committee also acknowledges that System Integration Labs are necessary to support testing of hypersonic weapon systems, specifically for the U.S. Army as it proceeds with the long range hypersonic weapon. Therefore, the

committee directs the Commander of U.S. Army Space and Missile Defense Command to provide a briefing to the House Committee on Armed Services not later than December 31, 2019, on capability and capacity assessments to support future ground testing. The briefing should include an analysis of integrated hardware and software processes and system integration and development.

Integrated Silicon-Based Lasers

The committee is aware that the Department of Defense's weapons platforms, such as aircraft and radars, are still largely burdened with difficult to install and maintain, slow, expensive, and heavy copper wire cabling. The Department's initial investments in Integrated Silicon-Based Lasers have identified opportunities for transforming the state-of-the-art in the manufacture of integrated photonics devices. Integrated Photonics, the use of light for applications traditionally addressed through electronics, is used in a wide range of areas including telecommunications; 5G cell towers; cell phones; military laser-based radars; data communications; sensing; and could be used to replace heavy coaxial cabling in aircraft with fiber optic cables that are significantly smaller and lighter.

The committee directs the Under Secretary of Defense for Research and Engineering to submit a report to the House Committee on Armed Services by April 30, 2020, on how future military and commercial applications could use integrated photonics to benefit from higher bandwidth of data transfer, faster data transmission, and lower energy loss due to optical fiber being more energy efficient and lower weight than copper.

Investments in Science and Technology

The Department of Defense's Science and Technology (S&T) ecosystem is complex and is comprised of agencies, offices, laboratories, federally funded research and development centers, university affiliated research centers, academic partnerships, test and evaluation entities, and partnerships with the private sector to include small businesses. The Department's S&T ecosystem is charged with delivering the best capabilities to the warfighter in the near-, mid-, and long-term.

However, Defense Planning Guidance issued by the Under Secretary of Defense for Policy has for many years mandated only a base of zero percent real growth in the annual S&T budget. The fiscal year 2020 budget request for S&T was only 2.7 percent of the Department of Defense's base budget request and only 3.2 percent above the fiscal year 2019 requested funding level. Adjusted for inflation, the fiscal year 2020 request was only 1 percent higher than the fiscal year 2019 budget request.

The committee is concerned that the lack of growth negatively impacts the ability of the Department to keep pace with the real-world cost increases in the S&T ecosystem, such as the ability to attract highly specialized technical labor like scientists and engineers with advanced degrees and PhDs, and maintain a technological edge.

The committee is disappointed that this year's Defense Planning Guidance removed the base requirement of zero percent real growth. The committee is concerned that future budgets will show negative real growth and the Department's investments in its future technological edge will be even more dire. Therefore, the committee directs the Director, Cost Assessment and Program Evaluation, with analytical and resource support from the Under Secretary of Defense for Research and Engineering, to conduct a study and provide a briefing to the House Committee on Armed Services not later than September 1, 2021, on the effects of the Department submitting future budget requests with negative real growth in the Department's funding for S&T efforts.

Joint Threat Warning System

The committee recognizes that the Joint Threat Warning System (JTWS) provides credible threat warning and intelligence information to special operations forces (SOF). The committee notes that this program has been critical to enhancing the situational awareness of SOF elements by alerting them to threats to the force and illuminating targeting opportunities. The committee is concerned that the program does not include an air-variant precision high frequency band capability. This gap in coverage exposes SOF operators to unknown threats and decreases their situational awareness. Therefore, the committee directs the Commander, U.S. Special Operation Command to provide a briefing to the House Committee on Armed Services not later than December 1, 2019, on efforts to address this critical air-variant high frequency gap in coverage.

Microelectronics

The committee recognizes that microelectronics technology provides critical capabilities to Department of Defense, other government organizations' systems, and the commercial marketplace. With China's declared policy and commitment of dominating microelectronics market by 2025, the committee remains concerned with the Department of Defense's long-term strategy to maintain supply chain integrity and assurance against counterfeit parts and ensure continued access to trusted microelectronics. The committee is also concerned about the Department of Defense's lack of a robust industrial base and domestic supply chain for radiation-hardened microelectronics. The Department relies extensively on weapon and communications systems that must operate in high ambient radiation levels for national security, surveillance, battlefield communications, and missile defense. While there have been a number of attempts to address the challenges associated with the domestic microelectronics industry, the onset of 5G and the national security concerns associated with use of commercial microelectronics devices in military and other sensitive national security systems have increased the immediacy and level of concern. The committee supported the requirement in section 231 of the National Defense Authorization Act for Fiscal Year 2017 (Public Law 114-328) requiring the development of a microelectronics strategy. However,

with the introduction and proliferation of 5G technologies, the strategy must be updated.

Therefore, the committee directs the Secretary of Defense to provide a briefing to the House Committee on Armed Services not later than February 15, 2020, on the Department's Trusted Microelectronics strategy. The briefing should include the original elements of the strategy including supplier base capacity and need for trusted, radiation-hardened and anti-tamper microelectronics, and also address how the onset of 5G technologies is changing the national security and commercial marketplace for trusted microelectronics.

Protecting Critical Technologies Task Force

According to a memorandum issued by the Secretary of Defense on October 24, 2018, "each year, it is estimated that American industry loses more than $600 billion to theft and expropriation. Far worse, the loss of classified and controlled unclassified information is putting the Department's investments at risk and eroding the lethality and survivability of our forces." Protection of classified and controlled unclassified information, and intellectual property, when appropriate, is necessary for the U.S. to maintain a warfighting advantage.

The committee believes that effective protection of appropriately designated information requires a comprehensive, data-based understanding of theft and exportation and that impacted entities, such as academia and the Defense Industrial Base, must be part of the Department's efforts to develop solutions. The committee further believes that privacy and civil liberties, as well as an open research environment, must not be compromised by efforts to protect information.

For example, the Department funds basic research that benefits greatly from the global science and technology ecosystem. National Security Decision Directive 189 on the National Policy on the Transfer of Scientific, Technical and Engineering Information from President Reagan's administration outlined that the products of "fundamental research," defined as "basic and applied research in science and engineering, the results of which ordinarily are published and shared broadly within the scientific community," should remain unrestricted.

The committee is aware the Protecting Critical Technologies Task Force (PCTTF), established by former Secretary of Defense James Mattis, is one of the entities in the Department leading the effort to mitigate the loss of classified and controlled unclassified information. The committee supports the PCTTF and expects to be continually updated on its efforts. Additionally, the committee directs the Director of the PCTTF to provide a briefing to the House Committee on Armed Services not later than October 30, 2019, on efforts and progress to date.

TITLE V—MILITARY PERSONNEL POLICY

ITEMS OF SPECIAL INTEREST

Report on Integration of Women into Previously Closed Special Operations Forces Career Fields and the 75th Ranger Regiment

On January 13, 2016, U.S. Special Operations Command (SOCOM) Commander Joseph Votel issued a memo entitled "US Special Operations Command Implementation Plan for the Integration of Women." This memo detailed SOCOM's plan for the integration of women into the 75th Ranger Regiment and the eight special operations career fields previously closed to women, in accordance with former Secretary of Defense Ash Carter's decision to fully integrate women in the Armed Forces. The committee understands that the four lines of effort outlined in the SOCOM implementation plan, including Accession, Talent Management, Communication, and the Longitudinal Implementation Plan Assessment, remain in effect. However, the committee has yet to receive substantive information regarding the efforts relating to and progress towards integration of women into previously closed special operations career fields and the 75th Ranger Regiment.

Therefore, the committee directs the Commander of SOCOM to submit a report to the congressional defense committees not later than January 31, 2020, detailing efforts relating to and progress towards integration of women into the eight previously closed special operations career fields and the 75th Ranger Regiment since the issuance of the memorandum. The report shall include, but not be limited to, a description of efforts by SOCOM and its service component commands to recruit qualified female candidates; the number of qualified female candidates, by component command, that were selected to participate in initial selection, assessment, and qualification programs since 2016; the number of female candidates, by component command, that qualified for subsequent phases of training; the number of females in operational units; a description of the status of the four lines of effort; and any other matters the Commander of SOCOM deems relevant.

TITLE X—GENERAL PROVISIONS

ITEMS OF SPECIAL INTEREST

OTHER MATTERS

Evaluation of Integration of a Geographic Combatant Command and Theater Special Operations Command

Theater Special Operations Commands (TSOCs) are subunified commands of U.S. Special Operations Command (SOCOM) that are operationally controlled by geographic combatant commanders (GCC). The TSOC plans and conducts campaigns in support of the GCC across the spectrum of military operations.

The committee is concerned that GCC and TSOC organizational structures may not be optimal for managing, integrating, and synchronizing special operations

forces (SOF) operations across an area of responsibility (AOR). For example, GCC and TSOC mission, planning, and operational control misalignment was highlighted in the investigation of the October 2017 incident in Niger in which four U.S. service members were killed. Additionally, U.S. Africa Command recently completed an effort directed by the Secretary of Defense to review the SOF footprint in the AOR referred to as "optimization." The committee understands this effort was to decrease the reliance on SOF and more appropriately align SOF activities with GCC objectives. However, the committee believes that synchronization and alignment of SOF activities and operations to clear and concise GCC missions, goals, and objectives should be an ongoing priority for all GCCs, not directed by the Secretary of Defense.

Furthermore, according to recent work conducted by the Government Accountability Office (GAO) regarding SOF readiness, the operational tempo for SOF continues to be high due to an ever-increasing demand for forces by GCCs. A significant percentage of the demand is generated directly by the TSOCs, which set forth requirements for SOF in a relatively unconstrained manner. The committee notes this demand impacts the sustainability of current missions and SOF preparedness for future crises and conflicts.

The committee understands that as the Department of Defense focuses on near-peer competition, SOF will play a key role in such efforts, including in the U.S. European Command (EUCOM) AOR to address Russian malign influence. The committee notes that the percentage of SOF personnel deployed to Europe has grown significantly over the last several years and believes that the alignment of the GCC and TSOC is imperative for effective operations as well as to managing geopolitical and force protection risk related to any operations.

Therefore, the committee directs the Comptroller General of the United States to submit a report to the congressional defense committees by March 1, 2020, containing an assessment of the following: the sufficiency of EUCOM and U.S. Special Operations Command-Europe command structures to manage, integrate, and synchronize SOF operations in Europe; EUCOM's defined missions, goals, and objectives for SOF units operating in Europe and what challenges, if any, do units face measuring progress against those goals and objectives; SOCOM's ability to provide SOF required to support EUCOM and what impact, if any, has such resourcing had on the ability of SOF to carry out other ongoing or future operations; and any other issues the Comptroller General determines appropriate with respect to SOF operations in Europe.

Operational Use of Publicly Available Information

Violent extremist organizations and state-actors continue to conduct influence, command and control, and other overt operations in the information environment (IE), including on social media platforms, to achieve objectives that undermine U.S. national security. As such, the demand for the operational use of Publicly Available Information (PAI) for traditional military activities such as

military information support operations, battlespace awareness, and force protection continues to increase. In fact, the 2016 Department of Defense Strategy for Operations in the IE correlates information operations and cyberspace operations with the operational use of PAI.

The committee is aware that the collection, exploitation, understanding, and use of PAI may serve operational or intelligence operations or activities of the Department. The committee acknowledges that obtaining, understanding, and utilizing PAI for operational purposes presents significant and unique policy challenges. For example, the committee believes that protection of privacy and civil liberties of U.S. persons must remain a priority when setting forth guidance on accessing, acquiring, requesting, storing, analyzing, or otherwise using PAI for operational means, and that operational use of PAI should not serve as a replacement for Open Source Intelligence or other intelligence sources and tradecraft, or operational methods, for verifying military targets.

The committee notes that the Department has not yet established, but is formulating, a policy and governance structure for PAI. The committee is concerned that the lack of policy and governance structure is hindering the Department from maintaining an edge in and outside of the IE. The committee also notes that cover requirements and resources for administering cover may not be conducive to responsible and expedient operational use of PAI.

Therefore, the committee directs the Under Secretary of Defense for Policy, in coordination with the Under Secretary of Defense for Intelligence, to provide a briefing to the House Committee on Armed Services not later than October 1, 2019, on the operational use of PAI. The briefing shall include a description of the traditional military activities that may be enabled or enhanced using PAI, an update on policy formulation and considerations, frameworks for oversight and governance, cover requirements and guidance, and protection of U.S. persons privacy and civil liberties.

Special Operations Forces Professionalism and Ethics

In the committee report accompanying the National Defense Authorization Act for Fiscal Year 2018 (H. Rept. 115-200), the committee required the Department of Defense to provide a briefing containing an assessment of the culture and accountability of special operations forces (SOF) due to allegations of serious misconduct. Further, section 1066 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Public Law 115-232) required the Assistant Secretary of Defense for Special Operations and Low Intensity Conflict to conduct a review of ethics and professionalism programs available to SOF. This report was provided to the congressional defense committees on February 26, 2019, and reiterated the finding of a "disordered value system" that was identified by the Commander of U.S. Special Operations Command (SOCOM) after an internal survey of allegations of serious misconduct across the SOF enterprise in December 2018.

As a result of the survey findings, the former Commander of U.S. Special Operations Command, General Tony Thomas, outlined steps SOCOM would take over 90 days. This included a review of command climate surveys, reviewing programs of instruction, conducting research between trauma and behavioral health, and command level engagement with the force, to address the "disordered value system" focused on the individual and team rather than a commitment to serve.

The committee recognizes the efforts of senior SOF leadership to maintain and strengthen SOF ethos and urges the Commander of U.S. Special Operations Command and the Assistant Secretary of Defense for Special Operations and Low Intensity Conflict to continue such efforts. However, the committee has not been briefed on the results or continuing effort of the 90-day review and expects to be continually updated. Therefore, the committee directs the Commander of U.S. Special Operations Command, in coordination with the Assistant Secretary of Defense for Special Operations and Low Intensity Conflict, to provide a briefing to the House Committee on Armed Services not later than July 9, 2019, on the 90-day review and provide an update on other efforts relating to professionalism and ethics of the force.

TITLE XII—MATTERS RELATING TO FOREIGN NATIONS

ITEMS OF SPECIAL INTEREST

North Atlantic Treaty Organization Cooperative Cyber Defense Center of Excellence

The committee supports the efforts of the North Atlantic Treaty Organization (NATO) Cooperative Cyber Defense Center of Excellence (CCDCOE) and encourages the Department of Defense to collaborate fully with the Center. The committee notes that the CCDCOE can play a unique role by increasing and improving cyber cooperation, joint exercises, and policy development within NATO. Recent studies and analyses from the CCDCOE, such as the report on 5th Generation (5G) communications technologies and the report on Principles of Cyber Deterrence, are advancing important policy and technical conversations within NATO and across a broader technical community. However, the committee is concerned that an executive agent has yet to be appointed to serve as a proponent for the COE's important work. The committee urges the Department of Defense to continue to work with the interagency and utilize the CCDCOE to improve NATO's ability to counter and mitigate the threat of malign influence by Russian and other malign actors in cyberspace. The committee further encourages the CCDCOE to engage in research in enabling emerging technologies such as artificial intelligence, quantum computing, and other related areas.

Additionally, the committee directs the Secretary of Defense to provide a briefing to the House Committee on Armed Services not later than March 1, 2020, on ways

to improve cyber capabilities within NATO, including enhancing the capacity and resourcing of, and coordination with, the CCDCOE.

North Atlantic Treaty Organization Strategic Communications Center of Excellence

The committee supports the efforts of the North Atlantic Treaty Organization (NATO) Strategic Communications Center of Excellence (SCCOE), but remains concerned that the United States has not fully resourced or participated in this important COE. As the conferees noted in the conference report accompanying the National Defense Authorization Act for Fiscal Year 2018 (H. Rept. 115-404), by not actively participating, the Department of Defense is unable to shape the long-term agenda for research, exercises, and policy development. Furthermore, the Department is unable to embed personnel to gain experience or insight that can only be acquired by working side-by-side. The committee notes that the SCCOE can play a unique role by increasing cooperation for strategic communications within NATO and broader alliances, and provide research that directly addresses the many problems facing U.S. forces operating in the information environment. The committee urges the Department of Defense to work with the SCCOE and the interagency to improve NATO's ability to counter and mitigate disinformation, active measures, propaganda, and denial and deception activities of Russian and other malign actors. The committee further urges the Department of Defense to assign executive agent responsibilities to an appropriate organization within the Department of Defense to ensure effective partnering and advocacy for the COE.

Therefore, the committee directs the Secretary of Defense to provide a briefing to the House Committee on Armed Services not later than March 1, 2020, on ways to improve strategic communications within NATO, including enhancing the capacity of and coordination with the NATO Strategic Communications Center of Excellence.

TITLE XVI—STRATEGIC PROGRAMS, CYBER, AND INTELLIGENCE MATTERS

ITEMS OF SPECIAL INTEREST

CYBER-RELATED MATTERS

Briefing on the Integration of Cyber Planning at Unified Combatant Commands

The committee acknowledges U.S. Cyber Command's (CYBERCOM) efforts to develop and mature the Cyberspace Operations Integrated Planning Elements (COIPEs), teams of cyber operations planners from CYBERCOM who are forward staged at the unified combatant commands. While encouraged that CYBERCOM is seeking to integrate its planners at the geographic combatant commands and other functional combatant commands, the committee is concerned that this model could

be hampered by the same issues that plagued the Cyber Support Elements, a defunct CYBERCOM concept similar to the COIPEs that were first briefed to the committee in 2010. While these were operationalized at varying degrees, their deactivation and the subsequent need for COIPEs suggests the Cyber Support Element concept was executed poorly. Therefore, the committee directs the CYBERCOM Commander, in coordination with the Principal Cyber Advisor, to provide a briefing to the House Committee on Armed Services not later than January 31, 2020, on how the COIPEs are being organized, staffed, implemented, and utilized by the unified combatant commands. Additionally, the briefing will cover how the COIPE concept is distinctive from the Cyber Support Elements, and how the development of the COIPEs will avoid the problems encountered by the Cyber Support Elements.

Comptroller General Report to Study the Department of Defense's Current Inventory of Internet Protocol Version 4 Addresses

The committee directs the Comptroller General of the United States to submit a report to the congressional defense committees not later than March 1, 2020, on the Department of Defense's status and plans to transition from Internet Protocol version 4 (IPv4) to Internet Protocol version 6 (IPv6). The Comptroller General's report should assess:

(1) the technical and security necessity for the Department of Defense to transition from IPv4 to IPv6;

(2) any existing plans and requirements for transitioning from IPv4 to IPv6;

(3) the number and ranges of IPv4 addresses assigned to the Department of Defense;

(4) of those assigned, the address ranges that are unused by the Department of Defense;

(5) any statutory, policy, or security limitations that may preclude the Department of Defense's ability to transfer unutilized addresses;

(6) the ability of the Department of Defense to transfer IPv4 addresses upon transitioning to IPv6;

(7) estimated costs associated with transition to IPv6; and

(8) any other matters the Comptroller General determines appropriate.

Cyber Capability Development, Acquisition, and Sustainment

The committee supports the Department of Defense's objective of building a superior cyber force, which includes the acquisition, development, and sustainment of accesses and tools required to enable military cyber operations. However, the committee notes with concern the potential that the nation's cyber force could be hindered with tools and accesses being developed and stored by different components of the services and Department of Defense agencies and elements. For all the components under its authority, U.S. Cyber Command should maintain a

comprehensive and dynamic inventory of subordinate elements' accesses and tools, and emphasize the importance of sustaining these cyber-specific capabilities.

To this end, the committee directs the Secretary of Defense to provide a briefing to the House Committee on Armed Services not later than February 1, 2020, on the Department's strategy for acquisition, development, and sustainment of cyber-specific accesses and tools. This briefing should include details of the processes, procedures, roles and responsibilities, and sustainment plans for the Department of Defense's cyber capabilities. Additionally, the briefing should detail how the Department acquires tools, capabilities, and accesses from non-governmental sources, and conducts due diligence of these vendors.

Cybersecurity of the Supply Chain

The committee notes that effective and efficient supply chain management is critical for supporting the readiness and capabilities of the warfighter. U.S. Transportation Command (TRANSCOM), the Defense Logistics Agency (DLA), and the military services provide logistics capabilities that seek to deliver support to the warfighter at the right place, time, and cost. To meet this need, TRANSCOM, DLA, and the military services use information systems such as the Integrated Data Environment Global Transportation Convergence (IGC) database where 7,500 users have access to near-real time, in-transit visibility of 8 million lines of items of supply and transportation data.

The Department's Task Force on Survivable Logistics examined the threats posed by strategic competitors to military logistics and found that logistics information systems are potentially vulnerable to cyber attacks. The wide use of non-secure information technology across the logistics enterprise makes the military's systems potentially more susceptible to enemy activity as does the integration with commercial networks for suppliers and mobility. The task force also found that the Department has not conducted an end-to-end vulnerability assessment to remedy cyber challenges to logistics information systems that could be exploited in a strategic competition. Moreover, the Department does not have a corrective action plan to mitigate the potential risks associated with vulnerabilities in the logistics arena.

Therefore, the committee directs the Comptroller General of the United States to evaluate to what extent the Department has identified and addressed cybersecurity risks to its supply chain; to what extent the Department has visibility into cybersecurity risks to its supply chain for activities led by commercial networks and contractors; to what extent the Department has corrective action plans in place to mitigate cybersecurity risks associated with the supply chain; and any other related matters the Comptroller General considers appropriate.

The committee further directs the Comptroller General to provide a briefing to the House Committee on Armed Services not later than March 1, 2020, on preliminary findings of the Comptroller General's evaluation, and to present final results in a format and timeframe agreed to at the time of the briefing.

Efforts to Leverage Education Programs for the Department of Defense Cyber Workforce

The committee recognizes the challenges facing the Department of Defense in recruiting, training, retaining, and building its workforce for cyberspace operations. This is even more difficult as the country as a whole faces a cybersecurity workforce shortage of nearly 314,000 individuals as of April 2019. The committee is aware of the multiple programs at the primary, secondary, and postsecondary levels to encourage students to get involved with technology and cybersecurity, but the committee is concerned that the Department of Defense and the military services are not postured to leverage these efforts without expanding their visibility and awareness of all the various initiatives underway. The current recruitment efforts by the military services do not appear calibrated for the needs of the Department in building its cyberspace force.

Therefore, the committee directs the Secretary of Defense to provide a briefing to the House Committee on Armed Services not later than March 31, 2020, on the Department's efforts to leverage and invest in the educational programs directed at primary, secondary, and postsecondary levels that are best suited to contribute to the Department's cyber workforce. The briefing should include information about how the military services are tailoring recruitment efforts for cyber fields, including emerging areas such as artificial intelligence, software engineering, data sciences, quantum sciences, and other related cross-functional technology fields.

Military Cyber Operations and Activities with Allies and Partners

The 2018 National Defense Strategy states that alliances and partnerships are one of the key elements the Department of Defense must possess to complement and enhance its warfighting capabilities. Similarly, the 2018 Department of Defense Cyber Strategy states that the Department will work with allies and partners to contest cyber activity that could threaten U.S. military forces and missions and to counter the exfiltration of sensitive Department information. While conducting cyber operations with allies and partners can enhance our nation's security and that of our allies and partners, it could also present challenges such as differing national security priorities and policies, laws, changing allegiances, transparency, and classification issues.

Therefore, the committee directs the Comptroller General of the United States to provide the congressional defense committees with an assessment of current military cyber operations with allies and partners. The assessment should include examples of offensive, defensive, and counterintelligence cyberspace operations that the Department conducts with allies and foreign partners and associated funding authorities or gaps; the status of current agreements and partnerships with countries with which the Department conducts regular cyberspace operations, including cyber threat information-sharing efforts and agreements; what is known about benefits and challenges the Department experiences in conducting cyberspace

operations with allies and foreign partners and the extent to which the Department is taking action to address any challenges; the extent to which the Department considers and incorporates allies' and foreign partners' capabilities, laws, and policies into the planning process for cyberspace operations; and any other matters the Comptroller General determines to be relevant.

The committee further directs the Comptroller General to provide a briefing to the House Committee on Armed Services not later than March 1, 2020, on the Comptroller General's preliminary findings, and to present final results to the congressional defense committees in a format and timeframe agreed to at the time of the briefing.

Persistent Cyber Training Environment

The committee judges the training of the service members and civilians dedicated to cyberspace operations as paramount, and a critical component to the nation's supremacy in cyberspace. To ensure unity of effort and synchronization in training across the military services, U.S. Cyber Command is developing the Persistent Cyber Training Environment (PCTE), with the U.S. Army serving as the program's executive agent. In concept, PCTE will be a hybrid cloud-based training platform supporting individual sustainment training, team certification, and provide the foundation for a collective training network. The committee supports PCTE as the mechanism for training the military and civilian personnel involved in cyberspace operations to maintain their skills and certification required to continue to work on missions.

To ensure the development of the program aligns with the program objectives, the committee directs the Commander of U.S. Cyber Command, in coordination with the Secretary of the Army, to provide a briefing to the House Committee on Armed Services by January 31, 2020, on PCTE. This briefing must include details on PCTE's governance framework and structure, current and projected program requirements, and acquisition schedule and plan, as well as a demonstration of the platform.

Pilot Program Authority to Enhance Cybersecurity and Resiliency of Critical Infrastructure

The committee supports the ongoing relationship and collaboration between the Department of Defense and the Department of Homeland Security to enhance cybersecurity and resiliency of critical infrastructure, as evidenced by the pilot program authorized in section 1650 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Public Law 115-232). The committee believes that state and non-state adversaries continue to conduct cyber operations that hold critical infrastructure and key resources at risk, and notes with concern the under-use of this authority since both departments have yet to maintain a sustained and recurring relationship of technical personnel.

The committee is supportive of the signed memorandum of understanding (MOU) between the two departments, including an agreement to jointly prioritize high-value national functions and non-Department of Defense-owned mission-critical infrastructure deemed to be most important to the military. The committee views this aspect of the MOU as central to the complementary cybersecurity roles and missions of the Department of Defense and Department of Homeland Security, and notes that the Department of Defense's "defend forward" posture can inform and guide Department of Homeland Security efforts to anticipate adversary action and understand potential risks to critical infrastructure.

Therefore, in order to ensure maturation and development of a sustained and recurring relationship that enhances cybersecurity cooperation, the committee directs the Secretary of Defense to provide a report to the House Committee on Armed Services by March 2, 2020, on the use and implementation of the pilot program authorized in section 1650, including any implementation mechanisms, lines of effort, joint principles, and plans for maintaining a sustained and recurring relationship between the Department of Defense and the Department of Homeland Security after termination of the authority on September 30, 2022.

Report on Information Security and Endpoint Accounting

The committee notes that section 1653 of the National Defense Authorization Act for Fiscal Year 2017 (Public Law 114-328) required the Department of Defense to develop and enforce a new policy referred to as "comply-to-connect." In general, a comply-to-connect policy requires that a computer be in compliance with the network's configuration standards before it is allowed to participate in the network. A complementary concept is "continuous monitoring" and associated solutions which automatically detect and remediate vulnerabilities, primarily on endpoint devices such as computers and mobile phones.

The committee remains concerned that the Department of Defense still lags the private sector in accounting for endpoints connected to the Department of Defense Information Network (DODIN). Therefore, the committee directs the Chief Information Officer (CIO) of the Department of Defense to submit a report to the congressional defense committees by February 1, 2020, on implementation of the plan required by subparagraph (a)(1)(A) of section 1653 of Public Law 114-328. At a minimum, the report shall include:

(1) a detailed assessment of progress made to date towards implementing the plan;

(2) an explanation of any barriers the Department has encountered in its efforts to provide a comprehensive accounting of endpoints connected to the DODIN;

(3) an overview of how "comply-to-connect" and "continuous monitoring" relate to the overall cybersecurity strategy of the Department; and

(4) any other matters the CIO determines appropriate.

Report on Principal Cyber Advisor Resources and Manning

Section 2224 of title 10, United States Code, authorized the position of a Principal Cyber Advisor (PCA) to the Secretary of Defense, to counsel the Secretary specifically on military cyber forces and activities and supervise cyber activities related to offensive missions, defense of the United States, and defense of Department of Defense networks, including oversight of policy and operational considerations, resources, personnel, and acquisition and technology. Since 2017, this position has been held by the Assistant Secretary of Defense for Homeland Defense and Global Security (ASD GS&HD), a role which includes the oversight of the planning capability development, and operational implementation in the mission areas of countering weapons of mass destruction; cyber; space; defense continuity; mission assurance; defense support of civil authorities; and supervision of the homeland defense activities of the Department of Defense. Since the creation of the PCA position, the office of the PCA has benefited from having a uniformed member of the military services in either the O-7 or O-8 level serving as the Deputy PCA, allowing for a senior individual to maintain focus on the responsibilities on a full-time basis.

The committee notes with concern that the responsibilities of the PCA cannot be afforded the requisite focus of the ASD GS&HD when that individual must contend with so many competing priorities. Additionally, the committee is equally concerned by the decision of the Joint Staff to eliminate the requirement for a general officer/flag officer to serve as the Deputy PCA. With the ASD GS&HD responsible for so many high-priority issues, the ability to rely on the experience and perspective of a senior military officer has been incalculable and the committee does not believe that a civilian may contribute to a comparable degree.

Therefore, the committee directs the Secretary of Defense to provide a briefing to the House Committee on Armed Services not later than January 31, 2020, on the role of the Principal Cyber Advisor, the Office of the Principal Cyber Advisor, current staffing, and a justification for reallocation of a military general officer/flag officer. Specifically, the briefing should include an analysis of the position of the Deputy PCA and the role of the military services in staffing the position.

Shared Cybersecurity Services Program for the Department of Defense

The committee notes the success of the Shared Cybersecurity Services Program, an effort by the Department of Homeland Security to host select security services on behalf of other Federal departments and agencies. This model offered improved cybersecurity to smaller Federal components that may lack the expertise to fully manage a comprehensive information technology security program, particularly given the increasing cyber threat. The size, scale, and federated nature of the Department of Defense's information technology footprint is so substantial that a similar model of shared cybersecurity services could reduce cybersecurity risk. The committee directs the Department of Defense Chief Information Officer to provide a briefing to the House Committee on Armed Services not later than April

1, 2020, on the feasibility of a shared cybersecurity services effort for the Department of Defense.

Synchronizing the Department of Defense Emergency Operations Management Systems

The committee recognizes the challenge of emergency operations management, both domestically and abroad, necessitating the synchronization of both military and civilian organizations, components, and agencies. During a natural disaster or physical incident, the Department of Defense must be able to communicate and coordinate with local authorities as well as other Federal agencies in responding to and providing assistance. The ability for government entities across the Federal, State, and local levels to communicate through a proven, widely adopted software solution should be a primary consideration for the Department of Defense.

The committee believes the Department can improve how emergency operations management and preparation are synchronized across the Department and military services, and can ensure that various components avoid developing solutions indigenously when widely adopted technological solutions are commercially available. Furthermore, the committee is aware of currently contracted and available commercial off-the-shelf (COTS) platforms that provide a common operating picture, enabling State and local users (both public and private entities) to communicate effectively with Federal agencies with complete scalability and configurability.

Therefore, the committee directs the Secretary of Defense to provide a briefing to the House Committee on Armed Services not later than March 31, 2020, on the Department's efforts to deconflict the emergency operations management systems utilized by various components across the Department and military services, and utilization of COTS solutions.

Utility Resilience Planning to Support Cybersecurity Threats

The committee recognizes utility systems located on Department of Defense installations are increasingly being connected to the internet and monitored or operated through computer-controlled industrial control systems (ICS). The benefits of such connection can be improved utility efficiencies and utility management. At the same time, the connectivity can expose the Department's utility systems to threats such as cyber attacks on ICS.

The committee is aware that prior Government Accountability Office (GAO) reports have identified challenges with the Department's ability to protect ICS from cyber threats, which could result in system failure or disruption. For example, in 2015, GAO reported that the military services had taken actions to mitigate risks posed by utility disruptions and were generally taking steps in response to Departmental guidance related to utility resilience. Further, GAO reported that at that time, the Department was in the planning stages of implementing new

cybersecurity guidance to enhance the cybersecurity of ICS, but faced challenges in implementing the guidance. The Department subsequently directed the services and other Defense agencies to develop plans for identifying the goals, milestones, and resources needed to identify, register, and implement cybersecurity controls on facility-related ICS. However, the status of implementation of this direction remains unclear to the committee.

Therefore, the committee directs the Comptroller General of the United States to evaluate the extent to which the military departments have developed and implemented plans and associated guidance to enhance the cybersecurity of ICS and what, if anything, remains incomplete; the challenges the military departments have encountered in implementing relevant guidance to enhance the cybersecurity of ICS and how effectively the challenges have been overcome; how effectively the military departments implemented industry leading practices to enhance cybersecurity for ICS; and how effectively the military departments conduct tests of the cybersecurity of ICS and implement improvements to security to counter any weaknesses identified.

The committee further directs the Comptroller General to provide a briefing to the House Committee on Armed Services not later than March 1, 2020, on preliminary findings of the Comptroller General's evaluation and to present final results in a format and timeframe agreed to at the time of the briefing.

INTELLIGENCE MATTERS

China's Biological Weapons Program

The committee remains interested in ensuring the Defense Intelligence Enterprise is providing timely, accurate, and effective intelligence to support information needs of the Department of Defense, and is aware of a recent Government Accountability Office report on long-range emerging threats facing the United States that highlighted potential pursuit by near-peer competitors of biological weapons using genetic engineering and synthetic biology. Therefore, the committee directs the Under Secretary of Defense for Intelligence, in coordination with the Director of the Defense Intelligence Agency, to provide a briefing to the House Committee on Armed Services by November 1, 2019, on an assessment of China's current and projected biological weapons program, the risks presented to the joint force, and the mitigation strategies to protect U.S. military forces against said threats.

Congressional Intelligence Notifications

The Secretary of Defense maintains a responsibility to keep the congressional defense and intelligence oversight committees fully and currently informed of all defense intelligence capabilities and activities to support Department of Defense operational and strategic requirements. The committee is aware that the Under Secretary of Defense for Intelligence (USDI) issued a

memorandum in January 2017 providing guidance to defense intelligence components on the necessity of providing timely and accurate notifications to Congress of all defense intelligence and counterintelligence activities. The committee supports additional efforts to enhance the Department's ability to provide timely, comprehensive, and accurate congressional intelligence notifications of intelligence and counterintelligence activities by the defense intelligence components listed in the January 2017 memorandum.

Therefore the committee directs the Under Secretary of Defense for Intelligence to provide a briefing to the House Committee on Armed Services and the House Permanent Select Committee on Intelligence by October 4, 2019, on the Department's current congressional notification policies and procedures regarding defense intelligence activities and support by defense intelligence components supporting the Department of Defense. The briefing shall include plans to strengthen this notification process by the defense intelligence components, to include notifications of new and updated intelligence-sharing arrangements and Basic Exchange and Cooperation Agreements with second- and third-party international allies and partners to support Department of Defense requirements, and a description of current and planned coordination efforts with the interagency, specifically the Office of the Director of National Intelligence, to include any dispute resolution processes in regard to conflicting use of defense intelligence capabilities to support defense priorities and objectives.

Current and Future Staffing Requirements of the Joint Intelligence Operations Centers

The committee recognizes the evolving operational and strategic priorities of the Department of Defense will impact Defense Intelligence Enterprise capabilities and resources. The committee recognizes the ongoing efforts by the Under Secretary of Defense for Intelligence (USDI) to comply with the committee's direction specified by the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Public Law 115-232) to reduce and prevent imbalances in priorities and mitigate against insufficient or misaligned resources within the Defense Intelligence Enterprise.

While the committee supports the efforts by USDI to create efficiencies across the Defense Intelligence Enterprise organizations, to include the Service Intelligence Centers and combatant command Joint Intelligence Operations Centers, and enable those elements to plan and posture staffing requirements accordingly, the committee is concerned that the shifts in current and future resourcing are lacking coherence to support the global mandate of the Department.

Therefore, the committee directs the Under Secretary of Defense for Intelligence, in coordination with the Director of the Defense Intelligence Agency, to provide a briefing to the House Committee on Armed Services by December 27, 2019, on how the Office of the Under Secretary of Defense for Intelligence and the Defense Intelligence Agency are managing resourcing requirements to the

combatant command Joint Intelligence Operations Centers to meet current and future needs of the combatant commanders and the Department of Defense.

Cyber Intrusions of the Defense Industrial Base and Academic Institutions Affiliated with the Department of Defense

The committee is aware of ongoing cyber attacks targeting the defense industrial base (DIB) and academic institutions affiliated with the Department of Defense. The committee is interested in gaining a better understanding of actual versus unsubstantiated open-source reporting to ensure proper oversight and resourcing of defense industrial base and academia cybersecurity measures.

While the committee recognizes the critical roles and expertise provided by the DIB and those academic institutions providing the Department of Defense with expertise to support capability research and development, the committee is concerned about the security controls protecting these virtual networks, especially in light of continued reports of cyber intrusions affecting elements of the DIB and affiliated academic institutions. The committee recognizes the importance of dispelling erroneous reporting, yet remains committed to ensuring continued, trusted partnerships comprising the foundations of the DIB to ensure comparative advantage for the joint force against strategic competitors.

Therefore, the committee directs the Under Secretary of Defense for Intelligence, in coordination with the Director of National Intelligence, to submit a report to the House Committee on Armed Services by December 6, 2019, describing how the Department defines cyber intrusions, including hacks, probes, penetrations, breaches, and other similar activities. The report shall also detail cyber intrusions of the DIB and affiliated academic institutions that have resulted in the compromise and loss of critical information relating to Department of Defense capabilities, programs, and/or activities in calendar years 2017 and 2018. Further, the report shall also include date and length of intrusion to include all events resulting in loss of information; total numbers of events for probes, hacks, penetrations, and breaches, as well as identification of threat actors and methods; and assessment of the impact of the totality of compromised information.

Development and Integration of Project Maven Services into Department of Defense Activities

The committee believes in the importance of developing artificial intelligence capabilities to enhance and augment execution of Defense Intelligence Enterprise (DIE) activities in support of Department of Defense priorities. Activities such as Project Maven are important efforts to modernize intelligence tradecraft and develop capabilities that can create efficiencies across the DIE and enhance effectiveness of defense operations. However, the committee is concerned about the broad scope of Project Maven, and the totality of requirements increasingly levied against the activity, without a comprehensive understanding of the key milestones

to track and measure progress and alignment of Maven accomplishments against evolving Department capabilities and activities.

Therefore, the committee directs the Under Secretary of Defense for Intelligence to provide a briefing to the House Committee on Armed Services not later than January 3, 2020, on Project Maven's strategy for tracking and aligning the activity's milestones against key DIE efforts, such as the Defense Intelligence Agency's Machine-assisted Analytic Rapid-repository System (MARS) and continued development of Department of Defense advanced analytic tradecraft and foundational intelligence against advanced weapons systems and capabilities.

Explosive Ordnance Disposal Intelligence

The committee is concerned that the expertise of Explosive Ordnance Disposal (EOD) personnel is not adequately accessible and therefore not sufficiently utilized by the Defense Intelligence Enterprise and intelligence community to provide the combatant commands with the required intelligence to identify, combat, and deter violent extremism and other asymmetric threats.

Explosive ordnance represents all munitions, inclusive of improvised explosive devices, propellants, nuclear fission or fusion materials, and biological and chemical agents. The primary consumers for this type of information are the military tactical explosive ordnance disposal units that employ the data for threat identification and neutralization. However, the required analyses to determine appropriate render-safe capabilities require operational and strategic intelligence to process and analyze the data, and data management processes to promulgate the resulting information. The committee believes the Department of Defense should modernize the processes and procedures to more comprehensively track, manage, and coordinate the capability and capacity of EOD intelligence within the intelligence community and the Defense Intelligence Enterprise to support all levels of render-safe capabilities.

Therefore, the committee directs the Under Secretary of Defense for Intelligence, in coordination with the Director of National Intelligence, to provide a briefing to the House Committee on Armed Services and the House Permanent Select Committee on Intelligence by March 6, 2020, on the capability and capacity of EOD intelligence expertise across the Defense Intelligence Enterprise and intelligence community. The briefing shall include an assessment of the coordination and integration of defense and national intelligence capabilities and capacity against EOD intelligence requirements, to include a mitigation strategy to address any identified gaps or deficiencies, information-sharing challenges, or any other impediments to integration of EOD expertise across the defense and intelligence communities. The briefing shall also include an assessment of the technical skills needed to address EOD intelligence requirements, while identifying any gaps or deficiencies in current personnel hiring and training structures, and a long-term plan to develop proficiency of EOD intelligence expertise in the defense and intelligence communities.

Governance of Data and Service Acquisitions Supporting Defense Intelligence Requirements

The committee recognizes initiatives across the Defense Intelligence Enterprise to collect, analyze, and share data to support critical foundation intelligence mission needs though various modernization initiatives like Project Maven and the Machine-assisted Analytic Rapid-repository System (MARS). However, the committee is concerned there is a lack of coordination and alignment of individual activities ongoing throughout the enterprise.

The committee lacks a comprehensive understanding of how data, information, and services procured in support of defense intelligence requirements are tracked, governed, and made available across the enterprise. The committee is concerned that as defense intelligence organizations move to cloud-based data management infrastructures, there is not enough emphasis on deconflicting these efforts to maximize investment and use across the enterprise and foreign partner coalitions. The committee notes that every effort should be made to ensure acquisition strategies that support these procurements make these products and services available to the entire enterprise, including U.S. allies and partners.

Therefore, the committee directs the Under Secretary of Defense for Intelligence to provide a briefing to the House Committee on Armed Services not later than December 6, 2019, on an enterprise-level strategy for data, information, and services acquisitions. The briefing shall detail a strategy to ensure these acquisitions are widely available across the Defense Intelligence Enterprise, thus reducing duplicative investments and creating efficiencies in the acquisition and capability management process.

Information-Sharing Arrangements with India, Japan, and the Republic of Korea

International alliances and partnerships are critical to the pursuit and sustainment of the United States national security objectives, built upon foundations of shared values and intent. The committee recognizes the importance of the Department of Defense sharing information with international allies and partners in support of the planning and execution of the National Defense Strategy, as allies and third-party international partners enhance strategic stability across the Department's purview while increasing effectiveness of operations. The committee believes the mechanisms to share information across the "Five Eyes" alliance continue to mature through established exercises, exchange of personnel, and virtual data sharing, while that cooperation is potentially less robust with third-party partners.

The committee supports the roles and contributions of third-party partners such as India, Japan, and the Republic of Korea, and recognizes their ongoing contribution toward maintaining peace and stability in the Indo-Pacific region. The committee is interested in understanding the policies and procedures governing the collaboration and information sharing with India, Japan, the Republic of Korea, and

the "Five Eyes" alliance, and if opportunities exist to strengthen those arrangements.

Therefore, the committee directs the Under Secretary of Defense for Intelligence, in coordination with the Director of National Intelligence, to provide a briefing to the House Committee on Armed Services by December 1, 2019, on the benefits, challenges, and risks of broadening the information-sharing mechanisms between India, Japan, the Republic of Korea, and the "Five Eyes" alliance.

Intelligence Support to Defense Operations in the Information Environment

The committee supports Department of Defense efforts to improve capabilities and tradecraft to operate in the information environment. The committee is concerned about the Defense Intelligence Enterprise's (DIE) ability to provide the information operations community with all-source intelligence support, consistent with the support provided to operations in other domains.

Therefore, the committee directs the Under Secretary of Defense for Intelligence, in coordination with the Joint Staff Director for Intelligence and the Director of National Intelligence, to provide a briefing to the House Committee on Armed Services by November 1, 2019, on intelligence support to information operations. The briefing should include standardized defense intelligence lexicon for intelligence preparation of the battlefield for information operations, efforts to develop a process to ensure the full scope of emerging defense information operations threat requirements are structured to be addressed through the entirety of DIE capabilities, and how the Department perceives the future of defense operations in the information environment.

The briefing shall also include a description of how the national intelligence community, through the National Intelligence Priorities Framework, will account for a more dynamic use of defense intelligence capabilities to augment and enhance support to Department of Defense operations in the information environment.

Investments in Scientific and Technological Intelligence

The committee remains interested in the continued efforts of the Department of Defense to improve scientific and technological intelligence (S&TI) capabilities and tradecraft across the Defense Intelligence Enterprise. The committee recognizes S&TI is critical to strategic competition with near-peer competitors by ensuring comprehensive understanding of adversary capabilities and ability to inform development of joint force fifth-generation advanced weapons systems and other emerging technologies. Therefore, the committee directs the Under Secretary of Defense for Intelligence, in coordination with the Director of the Defense Intelligence Agency, to provide a briefing to the House Committee on Armed Services by December 6, 2019, on the alignment of current and planned Defense Intelligence Enterprise S&TI investments and activities to Department of Defense operational and strategic requirements. The briefing shall also include information

on how the Department of Defense will continue the maturation of S&TI capabilities and tradecraft across the Defense Intelligence Enterprise.

Qualitative Analysis of Adversary Development of Emergent Technologies

The committee believes the Department of Defense must ensure that the Defense Intelligence Enterprise is providing timely, accurate, and effective intelligence to support acquisition and development of advanced joint force military systems and capabilities to support strategic competition with near-peer competitors like Russia and China. The committee is also aware of a recent Government Accountability Office report on long-range emerging threats facing the United States that represented a whole-of-government consensus on long-term strategic challenges.

Therefore, the committee directs the Secretary of Defense, in coordination with the Chairman of the Joint Chiefs of Staff and the Director of the Defense Intelligence Agency, to provide a report to the congressional defense committees and the congressional intelligence committees by December 6, 2019, containing a technical description of U.S. joint force emergent capabilities, as well as a description of advancements made by strategic near-peer competitors in comparable emergent technologies, including but not limited to hypersonic weapons, rail gun technologies, quantum computing, and counter-space capabilities. The report should detail technical data of emergent systems and capabilities of the U.S. joint force and of adversary capabilities, to include program mission, objectives and drivers for these technologies, development milestones, capability effective defensive and strike ranges, known vulnerabilities and strengths, and expected completion dates for the United States and each of its near-peer adversaries.

Further, the committee directs the Secretary of Defense, in coordination with the Chairman of the Joint Chiefs of Staff and the Director of the Defense Intelligence Agency, to provide a briefing to the House Committee on Armed Services not later than November 1, 2019, on the initial findings in the report, including specific information that will be used to affect defense acquisition and development of joint force systems and capabilities to ensure that the United States maintains the capability to deter and address emerging threats.

Reviewing the Integrated Defense Intelligence Priorities

The committee notes that the Department of Defense is a major provider of intelligence capabilities to the intelligence community, as well as a major consumer of intelligence information. The committee is aware of the operational constraints on the joint force that using the National Intelligence Priorities Framework to guide the allocation of Defense Intelligence Enterprise assets presents, especially for those that are integral to warfighting functions. The committee is concerned that the Integrated Defense Intelligence Priorities (IDIP) activity is not providing the intelligence support to defense operations that section 922 of the National Defense Authorization Act for Fiscal Year 2014 (Public Law 113–66) intended. Therefore,

the committee directs the Under Secretary of Defense for Intelligence to provide a briefing to the House Committee on Armed Services by December 27, 2019, with the current status of the IDIP activity, how the IDIP highlights gaps in defense and national intelligence priorities, and the measures in place to mitigate these gaps. The briefing shall also include details on why the IDIP is distinct from the National Intelligence Priorities Framework, an activity in which IDIP customers currently participate. Finally, the briefing shall also include a recommendation on whether the Department of Defense will continue or suspend the IDIP requirement.

Tactical Exploitation of National Capabilities Program

The Tactical Exploitation of National Capabilities Program (TENCAP) serves as the centralized lead to identify and execute national intelligence cross-agency solutions to evaluate, enhance, prototype, and transition technologies across the national intelligence enterprise into military service systems and architectures to create tactical intelligence effects. The committee supports TENCAP and the flexibility these programs require to mature, but believes the Department of Defense must develop metrics for measuring the impact of affiliated and incubated programs, to more accurately capture which activities and capabilities have successfully transitioned to programs of record and substantiate effectiveness of the joint force. Further, the committee notes that failure is an intrinsic, and sometimes necessary, component of the innovation process, and does not necessarily view failure to transition to a program of record as a negative issue.

Therefore, the committee directs the Under Secretary of Defense for Intelligence, in coordination with the directors of the military service TENCAP offices, to provide a briefing to the House Committee on Armed Services not later than November 1, 2019, on the plan to develop, track, and evaluate metrics associated with the TENCAP program for those projects which transition to programs of record.

Transitioning the Function of Background Investigations to the Department of Defense

Presidential Executive Order 13869 transitions the background investigation functions of the Federal Government from the Office of Personnel Management (OPM), National Background Investigations Bureau, to the Department of Defense, Defense Counterintelligence and Security Agency. The committee recognizes the importance of ensuring timely and efficient background investigations to overcome workforce staffing challenges of cleared individuals across the whole of government and private sector, and to vet personnel who come into contact with the Department's personnel, installations, and technology. The committee is aware of the temporary establishment of the Personnel Vetting Transformation Office in the Office of the Under Secretary of Defense for Intelligence to manage the transition of this activity from OPM to the Department

and improve the processes and procedures related to vetting personnel for clearances across the whole of government and private sector.

However, the committee is concerned about the potential risks to personnel management and mission such a transfer may present, and believes that appropriate protections of civil liberties and privacy must be prioritized throughout the transition, through the implementation of modern and efficient vetting measures. The committee recognizes the Department's leadership, through sharing best practices with the Office of the Director of National Intelligence, in reforming the vetting process using modern techniques such as continuous evaluation, and expects regular updates on the Department's progress in addressing the current background investigations backlog.

Therefore, the committee directs the Under Secretary of Defense for Intelligence, in coordination with the Director of the Defense Counterintelligence and Security Agency, to provide a briefing to the House Committee on Armed Services by December 27, 2019, on how the Department of Defense will transfer the background investigation mission and establish an effective personnel vetting capability to provide for the security of the Department, while maintaining the civil liberties and privacy protections of personnel under consideration to receive a clearance.

Unified Air Force Airborne Signals Intelligence Enterprise

The committee notes the goal of the Air Force Airborne Signals Intelligence (SIGINT) Enterprise (ASE) program is to produce an integrated, service-wide, capability-focused SIGINT architecture and investment strategy for the U.S. Air Force (USAF). However, the committee observes that while investment in the ASE program has produced significant advances in Air Force SIGINT capability, particularly within the RC-135 Rivet Joint program, the establishment of a true integrated airborne SIGINT enterprise architecture continues to elude the USAF. The committee is aware that significant capability gaps exist in MQ-9 SIGINT sensor relevancy against current threats, and the Air Force has not yet successfully addressed vanishing vendor issues with the high-altitude Airborne Signals Intelligence Payload (ASIP) program. Additionally, the USAF has not yet achieved a unified enterprise for SIGINT processing, exploitation, and dissemination (PED), despite having a distributed technical architecture within both the RC-135 Rivet Joint and Air Force Distributed Common Ground System (AF-DCGS) programs. The committee believes the Under Secretary of Defense for Intelligence should lead synchronization efforts with the intelligence community to integrate like data sources to enable more comprehensive analysis and exploitation on behalf of the military services.

Therefore, the committee directs the Secretary of the Air Force to provide a report to the House Committee on Armed Services by March 1, 2020, containing the Air Force's vision, strategy, and implementation plan to utilize Air Force airborne SIGINT program resources to establish a unified airborne SIGINT enterprise based

on shared joint and intelligence community standards. The committee looks forward to additional clarification on how this enterprise will allow RC-135, U-2, RQ-4, MQ-9, Air Force DCGS SIGINT systems, and future SIGINT capabilities to operate as an integrated enterprise using cloud-based technologies and distributed crew concepts to directly deliver SIGINT data to the joint force from a global Air Force SIGINT system.