H.R. 6395—FY21 NATIONAL DEFENSE AUTHORIZATION BILL

SUBCOMMITTEE ON INTELLIGENCE AND EMERGING THREATS AND CAPABILITIES

SUMMARY OF BILL LANGUAGE 1

BILL LANGUAGE 10

DIRECTIVE REPORT LANGUAGE 59

SUMMARY OF BILL LANGUAGE

Table Of Contents

DIVISION A—DEPARTMENT OF DEFENSE AUTHORIZATIONS

TITLE II—RESEARCH, DEVELOPMENT, TEST, AND EVALUATION

LEGISLATIVE PROVISIONS

SUBTITLE B—PROGRAM REQUIREMENTS, RESTRICTIONS, AND LIMITATIONS

Section 212—Pilot Program on Talent Optimization

Section 214—Extension of Pilot Program for the Enhancement of the Research, Development, Test, and Evaluation Centers of the Department of Defense

Section 215—Modification of Joint Artificial Intelligence Research, Development, and Transition Activities

Section 217—Social Science, Management Science, and Information Science Research Activities

Section 218—Board of Directors for the Joint Artificial Intelligence Center

Section 219—Directed Energy Working Group

SUBTITLE C—PLANS, REPORTS, AND OTHER MATTERS

Section 231—Modification to Annual Report of the Director of Operational Test and Evaluation

TITLE XII—MATTERS RELATING TO FOREIGN NATIONS

LEGISLATIVE PROVISIONS

SUBTITLE E—MATTERS RELATING TO THE INDO-PACIFIC REGION

Section 1243—Implementation of GAO Recommendations on Preparedness of United States Forces to Counter North Korean Chemical and Biological Weapons

TITLE XVI—STRATEGIC PROGRAMS, CYBER, AND INTELLIGENCE MATTERS

LEGISLATIVE PROVISIONS

SUBTITLE B—DEFENSE INTELLIGENCE AND INTELLIGENCE-RELATED ACTIVITIES

Section 1613—Report on Risk to National Security Posed by Quantum Computing Technologies

SUBTITLE C—CYBERSPACE-RELATED MATTERS

Section 1621—Cyber Mission Forces and Cyberspace Operations Forces

Section 1623—Tailored Cyberspace Operations Organizations

Section 1625—Department of Defense Cyber Workforce Efforts

Section 1626—Reporting Requirements for Cross Domain Compromises and Exemptions to Policies for Information Technology

Section 1627—Assessing Private-Public Collaboration in Cybersecurity

Section 1628—Cyber Capabilities and Interoperability of the National Guard

Section 1629—Evaluation of Non-Traditional Cyber Support to the Department of Defense

TITLE XVII—REPORTS AND OTHER MATTERS

LEGISLATIVE PROVISIONS

SUBTITLE A—STUDIES AND REPORTS

Section 1701—Review of Support of Special Operations to Combat Terrorism

DIVISION A—DEPARTMENT OF DEFENSE AUTHORIZATIONS

TITLE II—RESEARCH, DEVELOPMENT, TEST, AND EVALUATION

LEGISLATIVE PROVISIONS

SUBTITLE B—PROGRAM REQUIREMENTS, RESTRICTIONS, AND LIMITATIONS

Section 212—Pilot Program on Talent Optimization

This section would direct the Under Secretary of Defense for Research and Engineering, acting through the Director of the Defense Innovation Unit, to conduct a pilot program to develop a talent optimization marketplace for military personnel in the Reserve and Guard Components.

Section 214—Extension of Pilot Program for the Enhancement of the Research, Development, Test, and Evaluation Centers of the Department of Defense

This section would extend the termination date by 5 years for the pilot program for the enhancement of the research, development, test, and evaluation centers of the Department of Defense established in section 233 of the National Defense Authorization Act for Fiscal Year 2017 (Public Law 114-328). The new pilot termination date would be September 30, 2027. This section would require the Secretary of Defense to submit a report to the congressional defense committees not later than 1 year after the date of the enactment of this Act on the status of the pilot program, to include: (1) which military departments are not participating in the program; (2) any issues that are preventing their participation; and (3) any offices or elements of the Department that may be responsible for their delay in implementation. This section would also correct the title of the Assistant Secretary of the Army for Acquisition, Logistics, and Technology.

The committee believes in the importance of demonstrating methods for the more effective development of technology and management of functions at the Department's science and technology reinvention laboratories, test and evaluation centers part of the Major Range and Test Facility Base, and at the Defense Advanced Research Projects Agency. The committee urges each of the military services and the Office of the Secretary of Defense to make the most of the extended timeframe for this important pilot program.

Section 215—Modification of Joint Artificial Intelligence Research, Development, and Transition Activities

This section would amend section 238 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Public Law 115-232) by assigning

responsibility for the Joint Artificial Intelligence Center (JAIC) to the Deputy Secretary of Defense and ensure data access and visibility for the JAIC.

Section 217—Social Science, Management Science, and Information Science Research Activities

This section would direct the Secretary of Defense to carry out a social, management, and information science research and development program to ensure the Department of Defense has access to innovation and expertise in social, management, and information science necessary for improving the effectiveness and efficiency of executing Department of Defense operational and management activities. This section would require the Secretary to submit a report by December 31, 2022, to the congressional defense committees on the program, in both a classified and unclassified format.

The committee recognizes that all national security challenges facing the United States require an understanding of the causes and consequences of human behavior and has supported the Department's efforts to expand collaboration with the academic social science community through the Minerva Research Initiative since its establishment in 2008. Maintaining the Nation's technological superiority in the face of threats from great powers, state and non-state actors, and individuals requires not only investing in physical sciences but also the integration of knowledge from cross-disciplinary research that explores the social, cultural, behavioral, political, historic, and religious drivers and impacts of today's increasingly complex global security environment.

At a time when peer and near-peer adversaries are increasingly employing elements of malign influence, disinformation, and predatory economics in concert with technological capabilities, the Department should be increasing its investment in social science research programs, not ending it. Three recent reports from the National Academies assessing social science programs and their impacts on national security and intelligence noted the ongoing contributions of Minerva, and recommended ways to increase outreach and dissemination of results to enhance the success of the program.

The committee urges the Department of Defense to implement the recommendations of the National Academies to strengthen ties between grantees and potential users of their research and increase visibility, tracking, and dissemination of the research results to the broader national security community. All military services should participate in the program and highlight their specific plans and outcomes in annual budget documentation, further increasing visibility of Minerva-funded research to the user community.

Section 218—Board of Directors for the Joint Artificial Intelligence Center

This section would direct the Secretary of Defense to create and resource a Board of Directors for the Joint Artificial Intelligence Center (JAIC), comprised of senior Department of Defense officials, as well as civilian directors not employed by

the Department of Defense. The objective would be to have a standing body over the JAIC that can bring governmental and non-governmental experts together for the purpose of assisting the Department of Defense in correctly integrating and operationalizing artificial intelligence technologies.

Section 219—Directed Energy Working Group

This section would establish a Directed Energy Working Group inside the Department of Defense to coordinate directed energy efforts across the military services, leverage shared research and development, eliminate redundant efforts, and expedite the operationalization of directed energy programs.

SUBTITLE C—PLANS, REPORTS, AND OTHER MATTERS

Section 231—Modification to Annual Report of the Director of Operational Test and Evaluation

This section would amend section 139(h)(2) of title 10, United States Code, by removing the sunset date for the annual report submitted by the Director of Operational Test and Evaluation. This section does not change or alter any authorities of the Director of Operational Test and Evaluation.

TITLE XII—MATTERS RELATING TO FOREIGN NATIONS

LEGISLATIVE PROVISIONS

SUBTITLE E—MATTERS RELATING TO THE INDO-PACIFIC REGION

Section 1243—Implementation of GAO Recommendations on Preparedness of United States Forces to Counter North Korean Chemical and Biological Weapons

This section would direct the Secretary of Defense to submit a plan not later than 1 year after the date of the enactment of this Act to the congressional defense committees to address the recommendations in the U.S. Government Accountability Office's (GAO) report on Preparedness of U.S. Forces to Counter North Korean Chemical and Biological Weapons (GAO-20-79C). This section would also require the Secretary to begin implementation of the plan not later than 18 months after the date of the enactment of this Act. The Secretary may decide not to implement one of the recommendations in the report, but must submit justification for why not, and what else the Department of Defense will do to address the conditions underlying the recommendation.

The committee is concerned by many issues highlighted by GAO, and believes the Department's preparedness for a significant state-level weapons of mass destruction event is wholly inadequate. The Department's men and women in

uniform must be trained and equipped to successfully operate and perform in a contaminated environment.

TITLE XVI—STRATEGIC PROGRAMS, CYBER, AND INTELLIGENCE MATTERS

LEGISLATIVE PROVISIONS

SUBTITLE B—DEFENSE INTELLIGENCE AND INTELLIGENCE-RELATED ACTIVITIES

Section 1613—Report on Risk to National Security Posed by Quantum Computing Technologies

This section would direct the Secretary of Defense to assess the threats and risks posed by quantum computing to national security systems as well as strategies, plans, and investments needed to mitigate risks toward these systems. This section would also require the Secretary of Defense to provide a report to the congressional defense committees not later than December 31, 2021.

SUBTITLE C—CYBERSPACE-RELATED MATTERS

Section 1621—Cyber Mission Forces and Cyberspace Operations Forces

This section would amend section 238 of title 10, United States Code, to reflect the need for consolidated budget displays for both the cyber mission forces, as well as the newly created cyber operations forces. Additionally, this would amend an existing requirement for the cyber and information technology budgets to be delivered to Congress in print and electronically, not later than 5 days after the release of the President's budget request.

Section 1623—Tailored Cyberspace Operations Organizations

This section would direct the Secretary of the Navy, in conjunction with the Chief of Naval Operations, to produce a study on the Navy Cyber Warfare Development Group, a small niche organization aligned to the Navy's service cyber component. This section also would authorize other military services and U.S. Special Operations Command to create counterpart organizations to Navy Cyber Warfare Development Group.

Section 1625—Department of Defense Cyber Workforce Efforts

This section would direct the Department of Defense Chief Information Officer to:

(1) study and expand the model used at the National Security Agency (NSA) that authorizes NSA employees to use up to 140 hours of paid time toward NSA cyber education efforts in local communities. This would explicitly authorize select Department of Defense civilians who are part of the Cyber Excepted Service to utilize paid time toward wider national efforts aimed at addressing the cyber workforce shortage;

(2) study and report, in conjunction with the military services, to the congressional defense committees on how the Training With Industry program can be strengthened and better utilized by the services; and

(3) study the synchronization between NSA GenCyber program and the Centers for Academic Excellence and report to the congressional defense committees on how the two programs can be better integrated and harmonized.

Section 1626—Reporting Requirements for Cross Domain Compromises and Exemptions to Policies for Information Technology

This section would direct the Secretary of Defense to report monthly to the congressional defense committees on all cross domain compromises within the Department of Defense Information Network. Additionally, this section would direct the Secretary of Defense to report biannually to the congressional defense committees on all current exemptions to information technology policies. The intent is to establish a baseline for legislative oversight on areas where the Department of Defense has accepted risk to its networks and systems.

Section 1627—Assessing Private-Public Collaboration in Cybersecurity

This section would assess the impact of the current Pathfinder initiatives, prospects for making existing Pathfinder pilots more robust, and whether and how to expand Pathfinder or similar models of public-private collaboration to other critical infrastructure sectors, particularly systemically important critical infrastructure. Developing institutional support for Pathfinder-type initiatives not only creates opportunities for increased collaboration across critical sectors, as prioritized by Federal departments and agencies, but will also buttress and accelerate nascent efforts and increase their chances of success.

Section 1628—Cyber Capabilities and Interoperability of the National Guard

This section would direct the Department of Defense to update existing policies to consider National Guard activities that could be performed and reimbursed under title 32, United States Code.

Section 1629—Evaluation of Non-Traditional Cyber Support to the Department of Defense

This section would direct the Secretary of Defense to assess the feasibility and need for a cyber reserve force, the composition of a reserve force, and the structure of a reserve force (e.g., a retainer model, a non-traditional reserve, auxiliary model).

TITLE XVII—REPORTS AND OTHER MATTERS

LEGISLATIVE PROVISIONS

SUBTITLE A—STUDIES AND REPORTS

Section 1701—Review of Support of Special Operations to Combat Terrorism

This section would direct the Comptroller General of the United States to conduct a comprehensive review of the history, currency, processes and procedures for transitioning or terminating the programs provided by such authority, and the potential future use of the authority under section 127e of title 10, United States Code, in continued support of special operations to combat terrorism.

BILL LANGUAGE

SEC. 212 [Log 71180]. PILOT PROGRAM ON TALENT OPTIMIZATION.

Section 2358b of title 10, United States Code, is amended by adding at the end the following new subsection:

''(e) PILOT PROGRAM ON TALENT OPTIMIZATION.—

''(1) IN GENERAL.—The Under Secretary of Defense for Research and Engineering, acting through the Director of the Defense Innovation Unit, shall carry out a pilot program to develop a software-based system that enables active duty military units to identify, access, and request support from members of the reserve components who have the skills and expertise necessary to carry out one or more functions required of such units.

''(2) ELEMENTS.—In carrying out the pilot program, the Director of the Defense Innovation Unit shall—

''(A) ensure that the system developed under paragraph (1)—

''(i) enables active duty units, in near real-time, to identify members of the reserve components who have the qualifications necessary to meet certain requirements applicable to the units;

''(ii) improves the ability of the military departments to access, on-demand, members of the reserve components who possess relevant experience; and

''(iii) prioritizes access to members of the reserve components who have private-sector experience in the fields identified in section (b);

''(iv) leverages commercial best practices for similar software systems;

''(B) recommend policies and legislation to streamline the use of members of the reserve components by active duty units; and

''(C) carry out such other activities as the Director determines appropriate.

''(3) TERMINATION.—The authority to carry out the pilot program under this subsection shall terminate on September 30, 2025.''.

SEC. 214 [Log 70927]. EXTENSION OF PILOT PROGRAM FOR THE ENHANCEMENT OF THE RESEARCH, DEVELOPMENT, TEST, AND EVALUATION CENTERS OF THE DEPARTMENT OF DEFENSE.

(a) IN GENERAL.—Section 233 of the National Defense Authorization Act for Fiscal Year 2017 (Public Law 114–328; 10 U.S.C. 2358 note) is amended—

(1) in subsection (e), by striking ''2022'' and inserting ''2027''; and

(2) in subsection (f)—

(A) by amending paragraph (1) to read as follows:

''(1) IN GENERAL.—Not later than one year after the date of the enactment of the National Defense Authorization Act for Fiscal Year 2021, the Secretary of Defense shall submit to the congressional defense committees a report on the status of the pilot program.''; and

(B) in paragraph (2), by adding at the end the following new subparagraph:

''(F) With respect to any military department not participating in the pilot program, an explanation for such nonparticipation, including identification of—

''(i) any issues that may be preventing such participation; and

''(ii) any offices or other elements of the department that may be responsible for the delay in participation.''.

(b) TECHNICAL AMENDMENT.—Effective as of December 23, 2016, and as if included therein as enacted, section 233(c)(2)(C)(ii) of the National Defense Authorization Act for Fiscal Year 2017 (Public Law 114–328; 10 U.S.C. 2358 note) is amended by striking ''Assistant Secretary of the Army for Acquisition, Technology, and Logistics'' and inserting ''Assistant Secretary of the Army for Acquisition, Logistics, and Technology''.

SEC. 215 [Log 71397]. MODIFICATION OF JOINT ARTIFICIAL INTELLIGENCE RESEARCH, DEVELOPMENT, AND TRANSITION ACTIVITIES.

Section 238 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Public Law 115–232; 10 U.S.C. 2358 note) is amended—

(1) in the section heading, by inserting ''**AND IMPROVEMENT OF THE JOINT ARTIFICIAL INTELLIGENCE CENTER**'' before the period at the end;

(2) in subsection (a)—

(A) in paragraph (1), by inserting ''acquire,'' before ''develop''; and

(B) by amending paragraph (2) to read as follows:

''(2) EMPHASIS.—The set of activities established under paragraph (1) shall include—

''(A) acquisition and development of mature artificial intelligence technology;

''(B) applying artificial intelligence and machine learning solutions to operational problems by directly delivering artificial intelligence capabilities to the Armed Forces and other organizations and elements of the Department;

''(C) accelerating the development, testing, and fielding of new artificial intelligence and artificial intelligence-enabling capabilities; and

''(D) coordinating and deconflicting activities involving artificial intelligence and artificial intelligence-enabled capabilities within the Department.''

(3) by amending subsection (b) to read as follows:

''(b) RESPONSIBLE OFFICIAL.—The Deputy Secretary of Defense shall be the official within the Department of Defense with principal responsibility for the coordination of activities relating to the acquisition, development, and demonstration of artificial intelligence and machine learning for the Department.''.

(4) by redesignating subsections (c) through (g) as subsections (d) through (h), respectively;

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

''(c) ORGANIZATION.—

''(1) ROLE OF JOINT ARTIFICIAL INTELLIGENCE CENTER.—The set of activities established under subsection (a)(1) shall be established within the Joint Artificial Intelligence Center.

''(2) AUTHORITY OF DEPUTY SECRETARY OF DEFENSE.—The Deputy Secretary of Defense shall exercise authority and direction over the Joint Artificial Intelligence Center.

''(3) AUTHORITY OF DIRECTOR.—The Director of the Joint Artificial Intelligence Center shall report directly to the Deputy Secretary of Defense.

''(4) DELEGATION.—In exercising authority and direction over the Joint Artificial Intelligence Center under subsection (a), the Deputy Secretary of Defense may delegate administrative and ancillary management duties to the Chief Information Officer of the Department of Defense, as needed, to effectively and efficiently execute the mission of the Center.'';

(6) in subsection (d), as so redesignated—

(A) in the matter preceding paragraph (1), by striking ''official designated under subsection (b)'' and inserting ''Deputy Secretary of Defense'';

(B) in paragraph (1), in the matter preceding subparagraph (A), by inserting ''acquire,'' before ''develop'';

(C) in the heading of paragraph (2), by striking ''DEVELOPMENT'' and inserting ''ACQUISITION, DEVELOPMENT,''; and

(D) in paragraph (2)—

(i) in the matter preceding subparagraph (A), by striking ''To the degree practicable, the designated official'' and inserting ''The Deputy Secretary of Defense'';

(ii) in subparagraph (A), by striking ''development'' and inserting ''acquisition, development,'';

(iii) by redesignating subparagraphs (H) and (I) as subparagraphs (J) and (K), respectively; and

(iv) by inserting after subparagraph (G), the following new subparagraphs:

''(H) develop standard data formats for the Department that—

''(i) aid in defining the relative maturity of datasets; and

''(ii) inform best practices for cost and schedule computation, data collection strategies aligned to mission outcomes, and dataset maintenance practices;

''(I) establish data and model usage agreements and collaborative partnership agreements for artificial intelligence product development with each organization and element of the Department, including each of the Armed Forces;'';

(7) in subsection (e), as so redesignated—

(A) by striking ''the official designated under subsection (b)'' and inserting ''the Director of the Joint Artificial Intelligence Center'';

(B) by striking ''subsection (c)'' and inserting ''subsection (d)'';and

(C) by adding at the end the following: ''At a minimum, such access shall ensure that the Director has the ability to discover, access, share, and reuse data and models of the Armed Forces and other organizations and elements of the Department of Defense and to build and maintain data for the Department.'';

(8) in subsection (f), as so redesignated—

(A) in paragraph (1)—

(i) in the matter preceding subparagraph (A), by striking ''official designated under subsection (b)'' and inserting ''Deputy Secretary of Defense''; and

(ii) in subparagraph (B), by striking ''designated official'' and inserting ''Deputy Secretary of defense''; and

(B) in paragraph (2), by striking ''designated official'' and inserting ''Deputy Secretary of Defense''; and

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

''(i) JOINT ARTIFICIAL INTELLIGENCE CENTER DEFINED.—The term 'Joint Artificial Intelligence Center' means the Joint Artificial Intelligence Center of the Department of Defense established pursuant to the memorandum of the Secretary of Defense dated June 27, 2018, and titled 'Establishment of the Joint Artificial Intelligence Center', or any successor to such Center.''.

SEC. 217 [Log 70904]. SOCIAL SCIENCE, MANAGEMENT SCIENCE, AND INFORMATION SCIENCE RESEARCH ACTIVITIES.

(a) ESTABLISHMENT.—The Secretary of Defense, acting through the Under Secretary of Defense for Research and Engineering, shall carry out a program of research and development in social science, management science, and information science.

(b) PURPOSES.—The purposes of the program required under subsection (a) are as follows:

(1) To ensure that the Department of Defense has access to innovation and expertise in social science, management science, and information science to enable the Department to improve the effectiveness and efficiency of the Department's operational and management activities.

(2) To coordinate all research and development within the Department in the fields of social science, management science, and information science.

(3) To enhance cooperation and collaboration on research and development in the fields of social science, management science, and information science among the Department of Defense and appropriate private sector and international entities that are involved in such research and development.

(4) To develop and manage a portfolio of research initiatives in fundamental and applied social science, management science, and information science that is stable, consistent, and balanced across relevant disciplines.

(5) To accelerate efforts to transition and deploy technologies and concepts derived from research and development in the fields of social science, management science, and information science into the Department of Defense, and to establish policies, procedures, and standards for measuring the success of such efforts.

(6) To collect, synthesize, and disseminate critical information on research and development in the fields of social science, management science, and information science.

(7) To support the missions and systems of the Department by developing the fields of social science, management science, and information science, including by supporting—

(A) appropriate research and innovation in such fields; and

(B) the development of an industrial base in such fields, including development of the fa-

cilities, workforce, and infrastructure that comprise such industrial base.

(c) ADMINISTRATION.—The Under Secretary of Defense for Research and Engineering shall supervise the planning, management, and coordination of the program under subsection (a).

(d) ACTIVITIES.—The Under Secretary of Defense for Research and Engineering, in consultation with the Secretaries of the military departments and the heads of relevant Defense Agencies, shall—

(1) prescribe a set of long-term challenges and a set of specific technical goals for the program, including—

(A) optimization of analysis of national security data sets;

(B) development of defense-related management innovation activities;

(C) improving the operational use of social science, management science, and information science innovations by military commanders and civilian leaders;

(D) improving understanding of the fundamental social, cultural, and behavioral forces that shape the strategic interests of the United States; and

(E) developing a Department of Defense workforce capable of developing and leveraging innovations and best practices in the fields of social science, management science, and information science to support defense missions;

(2) develop a coordinated and integrated research and investment plan for meeting near-term, mid-term, and long-term national security, defense-related, and Department management challenges that—

(A) includes definitive milestones;

(B) provides for achieving specific technical goals; and

(C) builds upon the investments of the Department, other departments and agencies of the Federal Government, and the commercial sector in the fields of social science, management science, and information science;

(3) develop plans for—

(A) the development of the Department's workforce in social science, management science, and information science; and

(B) enhancing awareness of social science, management science, and information science within the Department; and

(4) develop memoranda of agreement, joint funding agreements, and such other cooperative arrangements as the Under Secretary determines necessary for carrying out the program under subsection (a).

(e) GUIDANCE REQUIRED.—

(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Under Secretary of Defense for Research and Engineering shall develop and issue guidance for defense-related social science, management science, and information science activities, including—

(A) classification and data management plans for such activities; and

(B) policies for control of personnel participating in such activities to minimize the effects of the loss of intellectual property in social science, management science, and information science considered sensitive to the Federal Government.

(2) UPDATES.—Under Secretary of Defense for Research and Engineering shall regularly update the guidance issued under paragraph (4).

(f) RESEARCH CENTERS.—

(1) IN GENERAL.—The Secretary of each military department may establish or designate an entity or activity under the jurisdiction of such Secretary, which may include a Department of Defense Laboratory, to serve as a research center in the fields of social science, management science, and information science. Each such research center shall engage with appropriate public sector and private sector organizations, including academic institutions, to enhance and accelerate the research, development, and deployment of social science, management science, and information science within the Department.

(2) MINIMUM NUMBER.—The Secretary of Defense shall ensure that not less than one research center is established or designated under paragraph (1) by not later than 180 days after the date of the enactment of this Act.

(g) REPORT.—

(1) IN GENERAL.—Not later than December 31, 2022, the Secretary shall submit to the congressional defense committees a report on the program.

(2) FORM OF REPORT.—The report required under paragraph (1) may be submitted in unclassified or classified form.

SEC. 218 [Log 70936]. BOARD OF DIRECTORS FOR THE JOINT ARTIFICIAL INTELLIGENCE CENTER.

(a) ESTABLISHMENT.—The Secretary of Defense shall establish a Board of Directors for the Joint Artificial Intelligence Center.

(b) DUTIES.—The duties of the Board of Directors shall be the following:

(1) Provide strategic guidance to the Director of the Joint Artificial Intelligence Center.

(2) Advise the Secretary on matters relating to the development and use of artificial intelligence by the Department of Defense.

(3) Evaluate and advise the Secretary on ethical matters relating to the development and use of artificial intelligence by the Department.

(4) Conduct long-term and long-range studies on matters relating to artificial intelligence.

(5) Evaluate and provide recommendations to the Secretary regarding the Department's development of a robust workforce proficient in artificial intelligence.

(6) Assist the Secretary in developing strategic level guidance on artificial intelligence-related hardware procurement and supply-chain matters.

(7) Monitor and provide recommendations to the Secretary on computing power, usage, storage,

and other technical matters relating to artificial intelligence.

(c) MEMBERSHIP.—The Board of Directors shall be composed of the following members:

(1) The official within the Department of Defense to whom the Director of the Joint Artificial intelligence center directly reports.

(2) The Under Secretary of Defense for Policy.

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

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

(5) The Under Secretary of Defense for Intelligence and Security.

(6) The Under Secretary of Defense for Personnel and Readiness.

(7) Not more than five members from academic or private sector organizations outside the Department of Defense, who shall be appointed by the Secretary.

(d) CHAIRPERSON.—The chairperson of the Board of Directors shall be the official described in subsection (c)(1).

(e) MEETINGS.—The Board of Directors shall meet not less than once each fiscal quarter and may meet at

other times at the call of the chairperson or a majority of the Board's members.

(f) REPORTS.—Not later than September 30 of each year through September 30, 2024, the Board of Directors shall submit to the congressional defense committees a report that summarizes the activities of the Board over the preceding year.

(g) DEFINITIONS.—In this section:

(1) The term ''artificial intelligence'' has the meaning given that term in section 238(g) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Public Law 115–232; 10 U.S.C. 2358 note).

(2) The term ''Board of Directors'' means the Board of Directors established under subsection (a).

(3) The term ''Joint Artificial Intelligence Center'' means the Joint Artificial Intelligence Center of the Department of Defense established pursuant to the memorandum of the Secretary of Defense dated June 27, 2018, and titled ''Establishment of the Joint Artificial Intelligence Center'', or any successor to such Center.

(4) The term ''Secretary'' means the Secretary of Defense.

SEC. 219 [Log 71457]. DIRECTED ENERGY WORKING GROUP.

(a) IN GENERAL.—The Secretary of Defense shall establish a working group, to be known as the ''Directed Energy Working Group''.

(b) RESPONSIBILITIES.—The working group shall—

(1) discuss the current and planned directed energy programs of each of the military departments;

(2) make recommendations to the Secretary of Defense about establishing memoranda of understanding among the organizations and elements of the Department of Defense to coordinate directed energy activities using amounts authorized to be appropriated for research, development, test, and evaluation; and

(3) identify methods of quickly fielding directed energy capabilities and programs.

(c) HEAD OF WORKING GROUP.—The head of the working group shall be the Assistant Director of Directed Energy of the Office of the Under Secretary of Defense for Research and Engineering.

(d) MEMBERSHIP.—The members of the working group shall be appointed by not later than 60 days after the date of the enactment of this Act, as follows:

(1) One member from each military department, appointed by the Secretary of the military department concerned.

(2) One member appointed by the Under Secretary of Defense for Research and Engineering.

(3) One member appointed by the Under Secretary of Defense for Acquisition and Sustainment.

(4) One member appointed by the Director of the Strategic Capabilities Office of the Department of Defense.

(5) One member appointed by the Director of the Defense Advanced Research Projects Agency.

(e) REPORTS TO CONGRESS.—Not later than 180 days after the date of the enactment of this Act, and not less frequently than once every 180 days thereafter, the working group shall submit to the congressional defense committees a report on the progress of each directed energy program being developed or fielded by the Department of Defense.

(f) TERMINATION.—The working group under this section shall terminate four years after the date of the enactment of this Act.

Subtitle C—Plans, Reports, and Other Matters

SEC. 231 [Log 71450]. MODIFICATION TO ANNUAL REPORT OF THE DIRECTOR OF OPERATIONAL TEST AND EVALUATION.

Section 139(h)(2) of title 10, United States Code, is amended—

(1) by striking ''Engineering,,'' and inserting ''Engineering,''; and

(2) by striking '', through January 31, 2025''.

SEC. 1243. [LOG 71378] IMPLEMENTATION OF GAO RECOMMENDATIONS ON PREPAREDNESS OF UNITED STATES FORCES TO COUNTER NORTH KOREAN CHEMICAL AND BIOLOGICAL WEAPONS.

(a) PLAN REQUIRED.—

(1) IN GENERAL.—The Secretary of Defense shall develop a plan to address the recommendations in the U.S. Government Accountability Office's report entitled ''Preparedness of U.S. Forces to Counter North Korean Chemical and Biological Weapons'' (GAO-20-79C).

(2) ELEMENTS.—The plan required under paragraph (1) shall, with respect to each recommendation in the report described in paragraph (1) that the Secretary of Defense has implemented or intends to implement, include—

(A) a summary of actions that have been or will be taken to implement the recommendation; and

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

(b) SUBMITTAL TO CONGRESS.—Not later than one year after the date of the enactment of this Act, the Sec-

retary of Defense shall submit to the congressional defense committees the plan required under subsection (a).

(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 (a).

(2) EXCEPTION FOR IMPLEMENTATION OF CERTAIN RECOMMENDATIONS.—

(A) DELAYED IMPLEMENTATION.—The Secretary of Defense may initiate implementation of a recommendation in the report described in subsection (a)(1) 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 decide not to implement a recommendation in the report described in subsection (a)(1) 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 alternative actions the Secretary plans to take to address the conditions underlying the recommendation.

SEC. 1613.[Log 70965] REPORT ON RISK TO NATIONAL SECURITY POSED BY QUANTUM COMPUTING TECHNOLOGIES.

(a) REPORT.—

(1) REQUIREMENT.—Not later than December 31, 2021, the Secretary of Defense shall submit to the congressional defense committees a report containing an assessment of the current and potential threats and risks posed by quantum computing technologies. The Secretary shall conduct the assessment in a manner that allows the Secretary to better understand and prepare to counter the risks of quantum computing to national security.

(2) MATTERS INCLUDED.—The report under paragraph (1) shall include the following:

(A) An identification of national security systems that are vulnerable to current and potential threats and risks posed by quantum computing technologies.

(B) An assessment of quantum-resistant cryptographic standards, including a timeline for the development of such standards.

(C) An assessment of the feasibility of alternate quantum-resistant models.

(D) A description of any funding shortfalls in public and private efforts to develop such standards and models.

(E) Recommendations to counter the threats and risks posed by quantum computing technologies that prioritize, secure, and resource the defense of national security systems identified under subparagraph (A).

(b) BRIEFINGS.—During the period preceding the date on which the Secretary submits the report under subsection (a), the Secretary shall include in the quarterly briefings under section 484 of title 10, United States Code, an update on the assessment conducted under such subsection.

(c) FORM.—The report under subsection (a) may be submitted in classified form.

Subtitle C—Cyberspace-Related Matters

SEC. 1621.[Log 71138] CYBER MISSION FORCES AND CYBERSPACE OPERATIONS FORCES.

Subsection (a) of section 238, title 10, United States Code, is amended—

(1) in the matter preceding paragraph (1)—

(A) by striking ''The Secretary'' and inserting ''Not later than five days after the submission by the President under section 1105(a) of title 31 of the budget, the Secretary'';

(B) by inserting ''in both electronic and print formats'' after ''submit''; and

(C) by striking ''2017'' and inserting ''2021'';

(2) in paragraph (1), by inserting ''and the cyberspace operations forces'' before the semicolon; and

(3) in paragraph (2), by inserting ''and the cyberspace operations forces'' before the period.

SEC. 1623.[Log 70928] TAILORED CYBERSPACE OPERATIONS ORGANIZATIONS.

(a) IN GENERAL.—Not later than 120 days after the date of the enactment of this Act, the Secretary of the Navy, in conjunction with the Chief of Naval Operations, shall submit to the congressional defense committees a study of the Navy Cyber Warfare Development Group (NCWDG).

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

(1) An examination of NCWDG's structure, manning, authorities, funding, and operations.

(2) A review of organizational relationships both within the Navy and to other Department of Defense organizations, as well as non-Department of Defense organizations.

(3) Recommendations for how the NCWDG can be strengthened and improved, without growth in size.

(c) DESIGNATION.—Notwithstanding any other provision of law, the Secretary of the Navy shall designate the NCWDG as a screened command.

(d) RELEASE.—The Secretary of the Navy shall transmit the study required under subsection (a) to the secretaries of the military services and the Commander of United States Special Operations Command.

(e) EXEMPLAR.—The service secretaries and the Commander of United States Special Operations Command are authorized to establish counterpart tailored cyberspace operations organizations of comparable size to the NCWDG within the military service or command, respectively, of each such secretary and Commander. Such counterpart organizations shall have the same authorities as the NCWDG. Not later than 30 days after receipt by each of the service secretaries and the Commander under subsection (d) of the study required under subsection (a), each such service secretary and Commander, as the case may be, shall brief the congressional defense committees regarding whether or not each such service secretary or Commander intends to utilize the authority under this subsection.

SEC. 1625.[Log 71262] DEPARTMENT OF DEFENSE CYBER WORKFORCE EFFORTS.

(a) RESOURCES FOR CYBER EDUCATION.—

(1) IN GENERAL.—The Chief Information Officer of the Department of Defense, in consultation with the Director of the National Security Agency (NSA), shall examine the current policies permitting National Security Agency employees to use up to 140 hours of paid time toward NSA's cyber education programs.

(2) REPORT.—

(A) IN GENERAL.—Not later than 90 days after the date of the enactment of this Act, the Chief Information Officer shall submit to the congressional defense committees and the congressional intelligence committees a strategy for expanding the policies described in paragraph (1) to—

(i) individuals who occupy positions described in section 1599f of title 10, United States Code; and

(ii) any other individuals who the Chief Information Officer determines appropriate.

(B) IMPLEMENTATION PLAN.—The report required under subparagraph (A) shall detail

the utilization of the policies in place at the National Security Agency, as well as an implementation plan that describes the mechanisms needed to expand the use of such policies to accommodate wider participation by individuals described in such subparagraph. Such implementation plan shall detail how such individuals would be able to connect to the instructional and participatory opportunities available through the efforts, programs, initiatives, and investments accounted for in the report required under section 1649 of the National Defense Authorization Act for Fiscal Year 2020 (Public Law 116–92), including the following programs:

(i) GenCyber.

(ii) Centers for Academic Excellence – Cyber Defense.

(iii) Centers for Academic Excellence – Cyber Operations.

(C) DEADLINE.—Not later than 120 days after the submission of the report required under subparagraph (A), the Chief Information Officer of the Department of Defense shall

carry out the implementation plan contained in such report.

(b) IMPROVING THE TRAINING WITH INDUSTRY PROGRAM.—

(1) IN GENERAL.—Not later than 120 days after the date of the enactment of this Act, the Principal Cyber Advisor of the Department of Defense, in consultation with the Principal Cyber Advisors of the military services and the Under Secretary of Defense for Personnel and Readiness, shall submit to the congressional defense committees a review of the current utilization and utility of the Training With Industry (TWI) programs, including relating to the following:

(A) Recommendations regarding how to improve and better utilize such programs, including regarding individuals who have completed such programs.

(B) An implementation plan to carry out such recommendations.

(2) ADDITIONAL .—Not later than 90 days after the submission of the report required under paragraph (1), the Principal Cyber Advisor of the Department of Defense shall carry out the implementation plan required under paragraph (1).

(c) ALIGNMENT OF CYBERSECURITY TRAINING PROGRAMS.—

(1) IN GENERAL.—Not later than 120 days after the date of the enactment of this Act, the Secretary of Defense shall submit to the congressional defense committees a report containing recommendations on how cybersecurity training programs described in section 1649 of the National Defense Authorization Act for Fiscal Year 2020 can be better aligned and harmonized.

(2) REPORT.—The report required under paragraph (1) shall provide recommendations concerning the following topics and information:

(A) Developing a comprehensive mechanism for utilizing and leveraging the Cyber Excepted Service workforce of the Department of Defense referred to in subsection (a), as well as mechanisms for military participation.

(B) Unnecessary redundancies in such programs, or in any related efforts, initiatives, or investments.

(C) Mechanisms for tracking participation and transition of participation from one such program to another.

(D) Department level oversight and management of such programs.

SEC. 1626.[Log 70933] REPORTING REQUIREMENTS FOR CROSS DOMAIN COMPROMISES AND EXEMPTIONS TO POLICIES FOR INFORMATION TECHNOLOGY.

(a) COMPROMISE REPORTING.—

(1) IN GENERAL.—Effective beginning in October 2020, the Secretary of Defense and the secretaries of the military services shall submit to the congressional defense committees a monthly report in writing that documents each instance or indication of a cross-domain compromise within the Department of Defense.

(2) PROCEDURES.—The Secretary of Defense shall submit to the congressional defense committees 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 such committees in writing of any changes to such procedures at least 14 days prior to the adoption of any such changes.

(3) DEFINITION.—In this subsection, the term ''cross domain compromise'' means any unauthorized connection between software, hardware, or both designed for use on a network or system built for classified data and the public internet.

(b) EXEMPTIONS TO POLICY FOR INFORMATION TECHNOLOGY.—Not later than six months after the date of the enactment of this Act and biannually thereafter, the Secretary of Defense and the secretaries of the military services shall submit to the congressional defense committees a report in writing that enumerates and details each current exemption to information technology policy, interim Authority To Operate (ATO) order, or both. Each such report shall include other relevant information pertaining to each such exemption, including relating to the following:

(1) Risk categorization.

(2) Duration.

(3) Estimated time remaining.

SEC. 1627.[Log 70958] ASSESSING PRIVATE-PUBLIC COLLABORATION IN CYBERSECURITY.

(a) REQUIREMENT.—Not later than 120 days after the date of the enactment of this Act, the Secretary of Defense shall—

(1) conduct a review and assessment of any ongoing public-private collaborative initiatives involving the Department of Defense and the private sector related to cybersecurity and defense of critical infrastructure, including—

(A) the United States Cyber Command's Pathfinder initiative and any derivative initiative;

(B) the Department's support to and integration with existing Federal cybersecurity centers and organizations; and

(C) comparable initiatives led by other Federal departments or agencies that support long-term public-private cybersecurity collaboration; and

(2) make recommendations for improvements and the requirements and resources necessary to institutionalize and strengthen the initiatives described in subparagraphs (A) through (C) of paragraph (1).

(b) REPORT.—

(1) IN GENERAL.—The Secretary of Defense shall submit to the congressional defense committees a report on the review, assessment, and recommendations under subsection (a).

(2) FORM.—The report required under paragraph (1) may be submitted in unclassified or classified form, as necessary.

(c) DEFINITION.—In this section, the term ''critical infrastructure'' has the meaning given such term in section 1016(e) of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001 (42 U.S.C. 5195c(e)).

SEC. 1628.[Log 70944] CYBER CAPABILITIES AND INTEROPERABILITY OF THE NATIONAL GUARD.

(a) EVALUATION.—Not later than 180 days after the date of the enactment of this Act, the Secretary of Defense, in conjunction with the Chief of the National Guard Bureau, shall submit to the congressional defense committees, the Committee on Appropriations of the House of Representatives, and the Committee on Appropriations of the Senate a review of the statutes, rules, regulations, and standards that pertain to the use of the National Guard for the response to and recovery from significant cyber incidents.

(b) RECOMMENDATIONS.—The review required under subsection (a) shall address the following::

(1) Regulations promulgated under section 903 of title 32, United States Code, to allow the National Guard to conduct homeland defense activities that the Secretary of Defense determines to be necessary and appropriate in accordance with section 902 of such title in response to a cyber attack.

(2) Compulsory guidance from the Chief of the National Guard Bureau regarding how the National Guard shall collaborate with the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security and the Federal Bureau of Investigation of the Department of Justice through

multi-agency task forces, information-sharing groups, incident response planning and exercises, and other relevant forums and activities.

(3) A plan for how the Chief of the National Guard Bureau will collaborate with the Secretary of Homeland Security to develop an annex to the National Cyber Incident Response Plan that details the regulations and guidance described in paragraphs (1) and (2).

(c) DEFINITION.—The term ''significant cyber incident'' means a cyber incident that results, or several related cyber incidents that result, in demonstrable harm to—

(1) the national security interests, foreign relations, or economy of the United States; or

(2) the public confidence, civil liberties, or public health and safety of the American people.

SEC. 1629.[Log 70945] EVALUATION OF NON-TRADITIONAL CYBER SUPPORT TO THE DEPARTMENT OF DEFENSE.

(a) REQUIREMENT.—Not later than 270 days after the date of the enactment of this Act, the Principal Cyber Advisor to the Secretary of Defense, in conjunction with the Under Secretary for Personnel and Readiness of the Department of Defense and the Principal Cyber Advisors of the military services, shall complete an assessment and evaluation of reserve models tailored to the support of cyberspace operations for the Department.

(b) EVALUATION COMPONENTS.—The assessment and evaluation required under subsection (a) shall include the following components:

(1) A current assessment of reserve and National Guard support to Cyber Operations Forces.

(2) An enumeration and evaluation of various reserve, National Guard, auxiliary, and non-traditional support models which are applicable to cyberspace operations, including a consideration of models utilized domestically and internationally.

(3) A utility assessment of a dedicated reserve cadre specific to United States Cyber Command and Cyber Operations Forces.

(4) An analysis of the costs associated with the models evaluated pursuant to paragraph (2).

(5) An assessment of the recruitment programs necessary for implementation of the models evaluated pursuant to paragraph (2).

(b) REPORT.—

(1) IN GENERAL.—The Secretary of Defense, acting through the Principal Cyber Advisor of the Department of Defense, shall submit to the congressional defense committees a report on the assessment and evaluation required under subsection (a).

(2) FORM.—The report required under paragraph (1) may be submitted in classified or unclassified form, as necessary.

Subtitle A—Studies and Reports

SEC. 1701 [Log 70971]. REVIEW OF SUPPORT OF SPECIAL OPERATIONS TO COMBAT TERRORISM.

(a) REVIEW.—The Comptroller General of the United States shall conduct a review of all support provided, or planned to be provided, under section 127e of title 10, United States Code. Such review shall include an analysis of each of the following:

(1) The strategic alignment between such support and relevant Executive Orders, global campaign plans, theatre campaign plans, execute orders, and other guiding documents for currency, relevancy, and efficacy.

(2) The extent to which United States Special Operations Command has the processes and procedures to manage, integrate, and synchronize the authority under section 127e of title 10, United States Code, in support of the objectives and priorities specified by the documents listed in (a)(1) as well as the objectives and priorities of—

(A) the geographic combatant commands;

(B) theatre elements of United States Special Operations Command;

(C) relevant chiefs of mission and other appropriate positions in the Department of State; and

(D) any other interagency organization affected by the use of such authority.

(3) For the activities carried out pursuant to such authority, the extent to which United States Special Operations Command has the processes and procedures to—

(A) determine the professionalism, cohesion, and institutional capacity of the military in the country where forces receiving support are based;

(B) determine the adherence of the forces receiving support to human rights norms and the laws of armed conflict;

(C) establish measures of effectiveness;

(D) assess such activities against established measures of effectiveness as identified in subparagraph (C);

(E) establish criteria to determine the successful completion of such activities;

(F) deconflict and synchronize activities conducted under such authority with other relevant funding authorities;

(G) deconflict and synchronize activities conducted under such authorities with other relevant activities conducted by organizations related to, but outside the purview of, the Department of Defense; and

(H) track the training, support, and facilitation provided to forces receiving support, and the significant activities undertaken by such forces as a result of such training, support, and facilitation.

(4) The extent to which United States Special Operations Command has processes and procedures to manage the sunset, termination, or transition of activities carried out pursuant to such authority, including—

(A) accountability with respect to equipment provided; and

(B) integrity of the tactics, techniques, and procedures developed.

(5) The extent to which United States Special Operations Command has and uses processes and procedures to—

(A) report to Congress biannually on the matters referred to in paragraph (3); and

(B) notify Congress with respect to the intent to sunset, terminate, or transition activities carried out pursuant to such authority.

(6) Any other issues the Comptroller General determines appropriate with respect to the authority under section 127e of title 10, United States Code.

(b) BRIEFING.—Not later than 180 days after the date of the enactment of this Act, the Comptroller General shall provide for the Committees on Armed Services of the Senate and House of Representatives a briefing on the progress of the review required under subsection (a).

(c) REPORT.—Not later than one year after the date of the enactment of this Act, the Comptroller General shall submit to the Committees on Armed Services of the Senate and House of Representatives a report on the findings of the review required under subsection (a) and the recommendations of the Comptroller General pursuant to such review.

(d) SUPPORT DEFINED.—In this section, the term ''support'' includes—

(1) personnel who provide capacity for—

(A) training and equipment;

(B) training, advice, and assistance; or

(C) advice, assistance, and accompaniment capacity;

(2) financial assistance; and

(3) equipment and weapons.

DIRECTIVE REPORT LANGUAGE

Table Of Contents

DIVISION A—DEPARTMENT OF DEFENSE AUTHORIZATIONS

TITLE II—RESEARCH, DEVELOPMENT, TEST, AND EVALUATION

RESEARCH, DEVELOPMENT, TEST, AND EVALUATION, AIR FORCE

Items of Special Interest

Air Force Institute of Technology research, development, test, and evaluation

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

Items of Special Interest

Department of Defense chemical and biological event response capabilities

Feasibility assessment of establishing large and open defense based data sets

High energy laser endless magazine definition

Implementation of Department of Defense Inspector General recommendations on additive manufacturing

Infrastructure to support research, development, test, and engineering at China Lake

Investment in research and development for technology to test treatments for nuclear, chemical, and biological exposure

Modular Open Systems common data standards

Public-Private Partnerships for Product Support on software-intensive government systems

TITLE V—MILITARY PERSONNEL POLICY

ITEMS OF SPECIAL INTEREST

Review of the Preservation of the Force and Family Program for Special Operations Forces

TITLE IX—DEPARTMENT OF DEFENSE ORGANIZATION AND MANAGEMENT

ITEMS OF SPECIAL INTEREST

Implementation of the Directed Roles and Responsibilities of the Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict

U.S. Special Operations Command Force Structure and Organization

TITLE X—GENERAL PROVISIONS

ITEMS OF SPECIAL INTEREST

OTHER MATTERS

Implementation of Findings and Recommendations of the 2020 U.S. Special Operations Command Comprehensive Review

Reserve Components and National Guard Units Supporting Special Operations Command Operational and Training Requirements

TITLE XII—MATTERS RELATING TO FOREIGN NATIONS

ITEMS OF SPECIAL INTEREST

North Korea's Chemical and Biological Weapons Capabilities

Report on Ties between Russia and China

TITLE XVI—STRATEGIC PROGRAMS, CYBER, AND INTELLIGENCE MATTERS

ITEMS OF SPECIAL INTEREST

CYBER-RELATED MATTERS

21st Century Integrated Digital Experience Act
Cyber Excepted Service
Cyber Mission Assurance Team Pilot Program
Department of Defense's Use of Efficient Peering Sites
Information Technology Asset Management and Inventory
Internet Architecture Security

INTELLIGENCE MATTERS

Department of Defense Artificial Intelligence Capabilities and Strategy
Joint Intelligence Brigade

DIVISION A—DEPARTMENT OF DEFENSE AUTHORIZATIONS

TITLE II—RESEARCH, DEVELOPMENT, TEST, AND EVALUATION

RESEARCH, DEVELOPMENT, TEST, AND EVALUATION, AIR FORCE

Items of Special Interest

Air Force Institute of Technology research, development, test, and evaluation

The committee recognizes the valuable contributions of the Air Force Institute of Technology (AFIT) to the professional development and technical expertise of the U.S. Air Force. The committee is aware of the continuing efforts of AFIT to provide cutting edge, specialized education to officer and enlisted U.S. military personnel and civilian employees in technical fields, including Aeronautics and Astronautics, Engineering Physics, and Systems Engineering. Despite the significant academic research that occurs at AFIT, it does not maintain a dedicated research, development, test, and evaluation (RDTE) program line. The committee is interested in understanding how AFIT may benefit from a dedicated RDTE line and what additional flexibility this may provide, including opportunities for expanded partnerships with other institutions of higher education and more influence over research topics that are of interest to the Department of Defense. Therefore, the committee directs the Secretary of the Air Force to provide a briefing to the House Committee on Armed Services not later than October 30, 2020, on the benefits and drawbacks of having a dedicated RDTE program line for the Air Force Institute of Technology.

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

Items of Special Interest

Department of Defense chemical and biological event response capabilities

At a time when the United States is struggling to respond to the spread of a highly infectious new virus, the committee is concerned about the preparedness of the U.S. Armed Forces to respond to a significant state-level weapons of mass destruction event. The Department of Defense's uniform and civilian personnel must be trained and equipped to successfully operate and perform in a contaminated environment. Therefore, the committee directs the Comptroller General of the United States to conduct a review of the Department's ability to respond to chemical and biological events. This review shall examine the extent to which the Department's military and chemical and biological defense support units, both around the world and in the United States, are prepared to counter chemical and biological weapons, including:

(1) detection and identification abilities;
(2) response plans;
(3) individual and collective protection;
(4) medical countermeasures and stockpile completeness;
(5) decontamination;
(6) response training and exercises;
(7) Department-wide tabletop exercises and wargames;
(8) research funding and partnerships with universities and the private sector; and
(9) any other matters the Comptroller General deems relevant.

The committee further directs the Comptroller General to provide a briefing to the House Committee on Armed Services by January 15, 2021, on the preliminary findings and to submit a final report on a date agreed to at the time of the briefing.

Feasibility assessment of establishing large and open defense based data sets

The committee believes that the Secretary of Defense should work with the Office of Science and Technology Policy (OSTP), the Office of Management and Budget (OMB), and the National Institute of Standards and Technology (NIST) to expand the number of open-source, high-quality data sets within Project Open Data to increase the availability of open data and foster research and innovation in data analytics, artificial intelligence, and machine learning. Therefore, the committee directs the Secretary of the Defense, in coordination with the Director of the Information Innovation Office at the Defense Advanced Research Projects Agency, to perform an assessment of large data sets maintained by the Department that could be publicly released for improved analytics and training of artificial intelligence and machine learning applications. The assessment shall include:

(1) a survey of the data sets maintained by the Department of Defense, to which artificial intelligence and machine learning is applicable, including but not limited to, health records; employment records; weather data; geospatial data; utilities; and logistics;

(2) necessary actions for the data sets identified in (1) to anonymize, sanitize, or otherwise remove sensitive information to make the data sets suitable for public consumption;

(3) the feasibility of releasing the resulting data sets of (2) through a public facing webpage;

(4) an assessment of the benefits resulting from the public availability of the data sets in (2), to include commercial, research, and government uses;

(5) an assessment of the benefit in developing the national security workforce resulting from the public availability of the data sets in (2) for use by K-12 and university education programs;

(6) a recommendation on the public release of the data sets in (2); and

(7) any other matters the Secretary determines appropriate.

The committee further directs the Secretary to submit a report to the Committees on Armed Services of the Senate and the House of Representatives not later than January 1, 2022, on the results of the assessment, and what engagement the Department has had with OSTP, OMB, and NIST on increasing the availability of open data.

High energy laser endless magazine definition

The committee supports investments across the Department of Defense in directed energy systems capable of countering the full array of incoming threats, from unmanned air systems to cruise missiles. The committee also supports development of systems with endless, or near endless, magazines to ensure capability to counter salvos or swarms of any size. The committee is concerned that while the Department has included reference to a near endless magazine in its budget justifications for high energy laser systems, it has not defined the term sufficiently to facilitate predictable requirements development and guide investment by industry.

The committee directs the Assistant Director for Directed Energy within the Office of the Under Secretary of Defense for Research and Engineering to submit a report to the House Committee on Armed Services by December 1, 2020, on the definition of an "endless magazine" to sufficiently facilitate predictable requirements development and guide investment by industry. The Assistant Director for Directed Energy shall assess whether, for high energy laser systems, an "endless magazine" shall be defined as an ability to engage at the rate necessary to counter highly complex, nearly simultaneous incoming threats, of the type for which the system was designed to counter, without temporary cessation of fire for battery recharge or exchange, thermal management, or other predictable technical limitations. The AD for DE shall provide a recommendation as to whether, except in the case of airborne applications, an endless magazine shall be provided as a stand-alone capability within the envelope of the platform, without the need for external devices or trailers.

Implementation of Department of Defense Inspector General recommendations on additive manufacturing

The committee is concerned with the Department of Defense's existing level of coordination of additive manufacturing efforts and encourages the use of additive manufacturing whenever possible to save both the Department and taxpayer valuable cost and time.

In October 2019, the Department of Defense Inspector General produced a report titled, "Audit of the DoD's Use of Additive Manufacturing for Sustainment Parts (DODIG-2020-003)," and provided a set of recommendations. The committee directs the Under Secretary of Defense for Research and Engineering, in coordination with the Under Secretary of Defense for Acquisition and Sustainment and the Service Acquisition Executives, to submit a report to the Committees on

Armed Services of the Senate and the House of Representatives by February 15, 2021, outlining the Department's plan to address each of the recommendations listed in the Inspector General report. Further, if the Under Secretary of Defense for Research and Engineering decides not to implement any of the Inspector General recommendations, they must include the justification for that decision in the report, as well what actions the Department will take to address the conditions underlying the recommendation.

Infrastructure to support research, development, test, and engineering at China Lake

The committee is aware of the significant research, development, test, and evaluation (RDT&E) infrastructure requirements across the Department of Defense. Section 252 of the National Defense Authorization Act for Fiscal Year 2020 (Public Law 116-92) requires the Secretary of Defense, in coordination with the Secretaries of the military departments, to complete a master plan of the current infrastructure needs of the Major Range and Test Facility Base not later than January 1, 2021. However, several Major Range and Test Facilities, including Naval Air Weapons Station (NAWS) China Lake, have more immediate requirements. NAWS China Lake performs a critical function for the Department of Defense, but was determined to be not mission capable after a 7.1 magnitude earthquake on July 5, 2019. In light of the importance of the mission and the investments made to date to repair NAWS China Lake, it is prudent that the committee fully understand the complete RDT&E infrastructure requirements before major construction commences. Therefore, the committee directs the Secretary of Defense to provide a briefing to the House Committee on Armed Services not later than October 30, 2020, on the RDT&E infrastructure master plan for NAWS China Lake.

Investment in research and development for technology to test treatments for nuclear, chemical, and biological exposure

As biological threats continue to advance, the committee encourages the Department of Defense to prioritize building on existing research and development to detect and model treatments for the potential aerosol dissemination of biological weapons. Areas for increased investment include, but are not limited to, the development of battlefield instrumentation and aerosol capabilities. The committee therefore directs the Deputy Assistant Secretary of Defense for Chemical and Biological Defense to provide a briefing to the House Committee on Armed Services not later than January 15, 2021, on the Department's assessment of organ-on-chips technology as a platform for threat assessment and for rapidly developed treatments (medical countermeasures) for biological, chemical, and radiological threats, and what plans the Department has to use this technology going forward.

Modular Open Systems common data standards

The committee continues to be encouraged by the development, demonstration, and validation of common data standards and implementation of the Modular Open Systems Approach. However, the committee is concerned that access to these standards by the general academic population and technology industry remains limited. The committee notes that while a subset of the components of these standards are based on sensitive or classified information, that the data standards and interfaces used by the Department are predominantly based on publicly available sources such as foundational science and engineering principles. The committee further notes that restricting public access to the portion of the standards based on public knowledge unnecessarily increases cost for the conversion of commercial products to defense applications and limits the experimentation and innovation available to the Department of Defense. The committee is concerned that barriers to accessing these standards have an outsized impact in the fields of artificial intelligence, autonomy, and unmanned air vehicles.

Accordingly, the committee directs the Secretary of Defense to provide a report to the House Committee on Armed Services not later than February 15, 2021, on:

(1) which components of the common data standards used by the Department are based on publicly available knowledge, to include, at a minimum: Open Mission Systems developed by the Air Force; the Future Airborne Capabilities Environment developed by the Navy; and the VICTORY Initiative, developed by the Army;

(2) the applicability of these components to artificial intelligence-based technologies, including autonomous ground vehicles or unmanned air vehicles;

(3) the feasibility of releasing a public subset of the data standards to reduce the barriers to research with, and adoption by, academia and technology companies;

(4) an assessment of the cost savings to the Department attributable to the public release of a subset of the data standards; and

(5) an assessment of the benefit in developing the national security workforce by releasing a public subset of the data standards.

Public-Private Partnerships for Product Support on software-intensive government systems

The committee notes the work of the Department of Defense in codifying Public-Private Partnerships for Product Support through Department of Defense Instruction 4151.21. This instruction requires that public-private partnerships (PPP) for depot-level maintenance be employed whenever it is cost-effective in providing improved support to the warfighter. The goal is to maximize the utilization of the government's facilities, equipment, and personnel at Department of Defense depot-level maintenance activities as a way to facilitate innovative and creative thinking.

However, it is evident that maintaining a conventional PPP as it relates to software-intensive systems further complicates the partnership and hinders the goal of a PPP to "ensure effective and timely response to mobilization, national defense contingency situations, and other emergency requirements." This is because risk is induced as software crosses multiple subsystems and can lead to complications for a program. Requiring different groups to perform routine updates on software that may have a commercial origin can cause system anomalies and duplication of effort. The current requirements from the Department of Defense Instruction 4151.21 appear ill-suited for application to the Department's software usage.

The committee supports the Department's efforts to prioritize partnerships between public and private entities to achieve critical, yet cost-effective support to the warfighter. However, the Department should reevaluate the requirements for the PPP as relates to software systems. Therefore, the committee directs the Secretary of Defense to provide a briefing to the House Committee on Armed Services not later than August 1, 2021, on how the Department of Defense can adjust requirements to make these more applicable to software systems.

TITLE V—MILITARY PERSONNEL POLICY

ITEMS OF SPECIAL INTEREST

Review of the Preservation of the Force and Family Program for Special Operations Forces

The committee recognizes the importance of the Preservation of the Force and Family (POTFF) program to support the personnel and dependents of U.S. Special Operations Command (USSOCOM), and is supportive of the command's initiatives to broaden focus across the pillars of POTFF to more comprehensively address the stressors and needs of those special operations forces (SOF) and their families.

While POTFF has historically focused on rehabilitating and maintaining the operator through physical therapy initiatives, the committee maintains interest in ensuring balance of investment throughout POTFF to wholly address the mental, physical, spiritual, and familial needs of SOF. The committee notes the additional investments for the other pillars of POTFF, and is encouraged by the use of emergent technologies such as machine learning/artificial intelligence (ML/AI) to facilitate development of neurocognitive mapping capabilities to more accurately capture the psychological data of SOF, with the intention of aligning proper emotional care as they maneuver throughout the special operations enterprise.

The committee also notes the recent effort to establish Smartabase as the preferred program to virtually track SOF participating in the POTFF program. The committee understands the intent to have Smartabase implemented at each Service Component and Theater Special Operations Command element of USSOCOM. The

committee is also aware that Smartabase is intended to manage data associated with USSOCOM's SOF Assessment Baseline and Reassessment System.

However, with these concerns in mind, and to ensure that the command is honoring SOF truth number one, "Humans are more important than hardware," the committee directs the Comptroller General of the United States to provide a report to the House Committee on Armed Services by January 29, 2021, on the history, current use, and future intent for the POTFF program. The report shall include:

(1) observations regarding the balance of emphasis put on the four pillars of the program;

(2) the use of ML/AI to accurately capture and track the neurocognitive data of SOF and virtual connectivity to ensure that data is easily shared as SOF move across the enterprise;

(3) an assessment of the interoperability and scalability of the Smartabase system; and

(4) opportunities to enhance the POTFF program, especially considering transitioning and retired SOF who might still require the specialty care as provided by the POTFF program.

TITLE IX—DEPARTMENT OF DEFENSE ORGANIZATION AND MANAGEMENT

ITEMS OF SPECIAL INTEREST

Implementation of the Directed Roles and Responsibilities of the Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict

The committee acknowledges the Department of Defense's recent efforts to accelerate implementation of the roles and responsibilities of the office of the Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict (ASD SO/LIC) pursuant to section 922 of the National Defense Authorization Act for Fiscal Year 2017 (Public Law 114-328). The committee appreciates the Secretary of Defense's commitment to establishing measures to augment the office of ASD SO/LIC, including the consolidation of ASD SO/LIC personnel at the Pentagon.

The committee is aware that the Secretary of Defense intends to issue a memo to the Department reaffirming the overall responsibilities of ASD SO/LIC for special operations administrative matters and reinforcing the administrative chain of command as delineated in sections 138 and 167 of title 10, United States Code, and is aware of efforts by the office of ASD SO/LIC to revise and to publish the SO/LIC charter (Department of Defense Directive (DODD) 5111.10). The committee supports the investment by the Secretary of Defense in the Office of ASD SO/LIC to ensure comprehensive civilian oversight for the planning, resourcing, and employment of special operations forces (SOF).

Therefore, the committee directs the Secretary of Defense to provide a briefing to the House Committee on Armed Services by October 30, 2020, on the

implementation of those roles and responsibilities as directed by section 922. The briefing shall include:

(1) a timeline and milestones for moving SO/LIC staff back into the Pentagon from the Mark Center;

(2) a timeline and milestones for revising and publishing the SO/LIC charter (DODD 5111.10); and

(3) an assessment of the Department's efforts to enhance objective civilian oversight of SOF.

U.S. Special Operations Command Force Structure and Organization

The committee recognizes that the threat environment continues to evolve, driving strategic and operational force posture deliberations across the Department of Defense. The 2018 National Defense Strategy highlighted the need for the Department to reconsider whether and to what extent the forces historically applied against the countering violent extremist (CVE) mission, such as those from U.S. Special Operations Command (USSOCOM), should be utilized to confront great power competition (GPC).

The committee understands that USSOCOM has seen record growth with investments in information operations and cyber, with end strength now in excess of 73,000. While the committee is aware of ongoing efforts by USSOCOM to optimize special operations forces (SOF) resourcing and investments to meet demand of the CVE and GPC missions, the committee is concerned with the command's expanding force structure, to include the size and influence of the theater special operations commands (TSOCs).

Therefore, the committee directs the Comptroller General of the United States to conduct a review of USSOCOM's structure and organization of those forces aligned or assigned to the command. The review shall evaluate:

(1) the extent to which the Department or USSOCOM established guidance regarding how and when joint task forces (JTFs), including special operations joint task forces, should be established;

(2) the extent to which the Department or USSOCOM defined roles and responsibilities of TSOCs versus JTFs with regard to planning for and conducting operations;

(3) the extent to which the Department or USSOCOM established guidance regarding the size, structure, composition, and resourcing of JTFs;

(4) the extent to which USSOCOM or its components established a JTF in support of a global combatant command (GCC) requirement, and what command, control, or communication challenges, if any, those efforts created; and

(5) any other issues the Comptroller General deems appropriate with respect to the establishment and resourcing of JTFs as they relate to USSOCOM or SOF applied against GCC requirements.

The committee further directs the Comptroller General to provide a briefing to the House Committee on Armed Services by November 27, 2020, on the

preliminary findings and to submit a final report on a date agreed to at the time of the briefing.

TITLE X—GENERAL PROVISIONS

ITEMS OF SPECIAL INTEREST

OTHER MATTERS

Implementation of Findings and Recommendations of the 2020 U.S. Special Operations Command Comprehensive Review

The committee appreciates the substantial efforts undertaken by the Commander, U.S. Special Operations Command (USSOCOM) in recent years to address the concerns regarding the ethics and professionalism of the special operations forces (SOF). The committee is aware of multiple incidents across USSOCOM in 2018 and 2019, and appreciates the Command's ongoing focus to address congressional concerns related to alleged incidents of unethical and unprofessional behavior by SOF.

The Command's most recent effort to review and report on the culture and ethics of SOF is a welcome development in better understanding the Command's challenges and intended mitigation efforts to re-calibrate the force to SOF core values. The release of USSOCOM's Comprehensive Review indicated that the Command had established conditions for the normalization of an organizational culture overly focused on SOF employment and mission accomplishment, which created the contexts or situations allowing for misconduct and unethical behavior to develop within the SOF enterprise, not just at individual and team level, but also throughout the chain of command.

The committee notes that the Comprehensive Review Team posited a number of findings and recommendations for action to mitigate such challenges, ranging from an internal review of Theater Special Operations Command elements to self-validate SOF requirements to re-calibrating the incentives and promotion criteria for SOF officers and enlisted personnel. As with prior reviews, the committee understands that implementation of sustainable change is often more difficult than identifying problems, and is encouraged by the establishment of a Comprehensive Review Implementation Team to action the recommendations from the Comprehensive Review (CR).

Therefore, the committee directs the Commander, USSOCOM, to provide a briefing to the House Committee on Armed Services by October 30, 2020, on the implementation strategy of the CR findings. The briefing shall include:

(1) prioritization of implementation of proposed actions;

(2) status of implementation of proposed actions;

(3) any challenges to implementing the proposed actions; and

(4) funding or resource impacts resulting from implementation of proposed actions.

Reserve Components and National Guard Units Supporting Special Operations Command Operational and Training Requirements

The committee notes U.S. Special Operations Command (USSOCOM) continues to make strides in identifying causes of and establishing mitigation strategies for high operational tempo, impacts on air and ground platforms, and the resulting readiness challenges affecting special operations forces (SOF). The January 2020 release of USSOCOM's Comprehensive Review of SOF Culture and Ethics indicated that USSOCOM has established conditions for a culture focused on SOF employment and mission accomplishment, which in some instances occurs at the expense of disciplined, predictable, and reliable SOF force generation. The committee is concerned that the heavy emphasis on SOF employment in support of geographic combatant command and joint force requirements places excessive burden on Active Duty military personnel and capabilities assigned to USSOCOM.

The committee is aware the Services' Reserve Components and Air and Army National Guard units provide support to the operational and training requirements of USSOCOM. The committee believes that as processes and procedures are implemented to improve readiness and increase dwell time for Active Duty SOF personnel, regular and transparent dialog with the chiefs of the armed services, the National Guard Bureau, and service components of USSOCOM is critical to ensure that all associated elements of the Reserve Components and National Guard are considered for relevant operational and training opportunities.

Therefore, the committee directs the Commander, USSOCOM, to submit a report to the House Committee on Armed Services by December 1, 2020, on the current utilization strategy of the Services' Reserve Component and Air and Army National Guard units in support of USSOCOM. The report shall include:

(1) for units, the type and associated component, including numbers of personnel and associated occupational specialties;

(2) for individual personnel, the occupational specialty, parent organization, and associated component;

(3) associated air or ground platforms, capabilities, and maintenance status;

(4) dates of utilization for operational or training requirements in the past 5 years;

(5) location where each unit or individual supported USSOCOM;

(6) training to validate the operational capability and readiness of the supporting unit or individual; and

(7) intent for future utilization of each unit.

TITLE XII—MATTERS RELATING TO FOREIGN NATIONS

ITEMS OF SPECIAL INTEREST

North Korea's Chemical and Biological Weapons Capabilities

The committee notes that the Department of Defense has acknowledged the threat North Korea poses to national security. The committee believes the Department of Defense should work to ensure adequate attention is given to North Korea's chemical and biological weapons capabilities and assess readiness of the United States to combat these emerging threats.

Therefore, the committee directs the Secretary of Defense to provide a briefing to the House Committee on Armed Services not later than October 30, 2020, on North Korea's chemical and biological weapons capabilities and an assessment of the Department's readiness to combat these emerging threats. The briefing shall include:

(1) an assessment of relationships North Korea has, and may have, that would aid in their procurement or development of chemical and biological weapons;

(2) an assessment of North Korean investments or projects likely, or with significant potential, to be converted into military assets;

(3) an assessment of North Korean investments or projects of greatest concern with respect to United States national security interests;

(4) a description of any North Korean investments or projects located in another country that is linked to military cooperation with such country;

(5) a summary of the North Korean chemical and biological weapons program, including research, development, production, weaponization, and delivery capabilities; and

(6) an assessment of the Department's current readiness, or deficiencies thereof, to counter a North Korean chemical or biological attack on the Korean Peninsula.

Report on Ties between Russia and China

The Department of Defense has acknowledged that China and Russia are increasingly working in cooperation on a wide range of matters, including economically, politically, and militarily; and that the Department believes the growing ties between Russia and China are challenging the rules-based order and present a threat to U.S. national security interests. The committee notes that the National Defense Strategy highlights the joint force's eroding competitive edge against China and Russia. The committee endeavors to fully understand the extent of the ties between Russia and China. Therefore, the committee directs the Director of National Intelligence, in consultation with the Secretary of Defense, to submit a report to the congressional defense committees and the congressional intelligence committees by March 1, 2021, on the relationship between China and Russia.

The report shall include:

(1) an assessment of the military relationship between Russia and China, including military exercises, arms sales, security agreements, and joint military educational exchanges;

(2) an assessment of the economic ties between Russia and China, including collaboration or cooperation on China's One Belt One Road initiative;

(3) an assessment of cultural exchanges between Russia and China;

(4) an assessment of the educational and professional exchanges between Russia and China, to include scientists, engineers, academics, and other technical professionals;

(5) an assessment of competing interests between Russia and China that limit collaboration and cooperation between the two countries; and

(6) an assessment of whether, and if so to what degree, cooperation between Russia and China is eroding the United States competitive edge or its influence around the world.

The report required shall be submitted in unclassified form, but may include a classified annex.

TITLE XVI—STRATEGIC PROGRAMS, CYBER, AND INTELLIGENCE MATTERS

ITEMS OF SPECIAL INTEREST

CYBER-RELATED MATTERS

21st Century Integrated Digital Experience Act

The 21st Century Integrated Digital Experience Act (IDEA) (Public Law 115-336), enacted in December 2018, required the Department of Defense to modernize internal digital services, intranets, and external websites, with the goal of improving the delivery of customer service to employees, Active Duty personnel, family members, and others that interact with the Department. In addition, Public Law 115-336 required that the Department make all paper-based forms related to serving the broader Department of Defense community, of which there are thousands, available in digital and mobile responsive format by December 2020.

The committee believes that embracing the requirements of 21st Century IDEA would have a significant positive impact on the Department's mission delivery and customer experience. Therefore, the committee directs the Secretary of Defense, in coordination with the Department of Defense Chief Information Officer, to provide a report to the House Committee on Armed Services not later than March 31, 2021, on the status of the Department's implementation of the 21st Century IDEA across the defense enterprise. Specifically, this report should include military department and unified command plans to meet the December 2020 forms modernization deadline, ensuring each department or command has a 21st Century

IDEA designee and plans to budget and comply with any deadlines the Department may have missed.

Cyber Excepted Service

In the committee report accompanying the National Defense Authorization Act for Fiscal Year 2020 (H. Rept. 116-120), the committee expressed concern at the slow pace of implementation of the Cyber Excepted Service (CES) personnel system, a component of the excepted service authorized in section 1588f of title 10, United States Code, aimed at recruiting and retaining highly trained cybersecurity professionals within the Department of Defense.

The committee is encouraged by the substantial progress the Department's Chief Information Officer (CIO) has made in implementing CES authorities across the Department. The committee recognizes the importance of bolstering the nation's cybersecurity workforce with professionals with backgrounds in machine learning, artificial intelligence, software development, and data science. CES authorities will allow the Department to effectively recruit and retain these highly skilled individuals and compete with the private sector for top talent, ensuring the Department's cyber workforce is ready and equipped to address current and future cyber threats.

As the CES continues to evolve across the Department, the committee expects to be kept informed on further maturation and implementation of CES hiring authorities. Therefore, the committee directs the CIO, as the executive agent responsible for the administration of CES, to provide a report to the House Committee on Armed Services by February 1, 2021, on the use of CES authorities across the Department of Defense, mechanisms for non-CES Department of Defense components to petition for inclusion, and applicability of interim security clearances for CES positions.

Cyber Mission Assurance Team Pilot Program

The committee applauds the National Guard Bureau for its Cyber Mission Assurance Teams (CMAT) pilot program, an effort designed to harness the cyber talent of the National Guard for the protection of critical infrastructure connected to military installations. Efforts such as the nascent CMAT program are important as the military services seek to better understand the operational risks, to include cybersecurity, of domestic installations. The capability developed can assist the National Guard, when utilized for operations under both title 32 and title 10, United States Code. The committee directs the Chief of the National Guard Bureau to present a comprehensive report to the House Committee on Armed Services not later than May 31, 2021, on the CMAT pilot program as well as the future direction of the effort. More specifically, the committee seeks greater fidelity on how the CMAT program will align to the Federal Emergency Management Agency's regional construct, as well as work with the Cybersecurity and Infrastructure Security

Agency's Critical Infrastructure Vulnerability Assessments program and the Protective Security Advisors program.

Department of Defense's Use of Efficient Peering Sites

The committee is aware of the importance of private network and cloud interconnection to address fragmented Department of Defense internet architecture and the ability to successfully migrate services to the cloud. The committee understands that the use of secure, advanced, internet exchange points mitigates cyber vulnerabilities, improves data security, increases system reliability and resilience, and reduces processing time latency. Therefore, the committee directs the Chief Information Officer of the Department of Defense to provide a briefing to the House Committee on Armed Services, not later than July 31, 2021, on the Department's deployment of private, low-latency network and cloud interconnection at global peering locations.

Information Technology Asset Management and Inventory

The committee commends the Department of Defense for the considerable improvement made on information technology, asset discovery, and asset management. However, the committee believes the Department would benefit from an established process for auditing software and hardware inventories. The lack of a single policy framework hinders the capacity of the Department to discover license duplication and the Department is at risk of wasting valuable resources on redundant or underutilized hardware and software. The private sector has successfully navigated this challenge through the use of automated software tools widely available on the commercial market.

The committee directs the Chief Information Officer of the Department of Defense, in coordination with chief information officers of the military services, to provide a briefing to the House Committee on Armed Services, not later than September 1, 2021, on the processes in place for asset discovery and management of hardware and software products. This briefing should present the following information:

(1) process for identifying duplicative software licenses;

(2) process for identifying redundant and/or duplicative software and hardware;

(3) process for identifying and cataloging usage information for both hardware and software; and

(4) process for identifying potential cost savings from the aforementioned briefing elements.

Internet Architecture Security

The committee recognizes that the internet is inextricable and central to the American way of life, and the architecture that enables internet communications is layered, complex, and multifaceted. The committee notes that this architecture includes high-capacity cables laid underground and underseas, cable landing stations that connect cables from continent to continent, and internet exchange points that serve as clearinghouses for data between Internet Service Providers and content delivery networks; all of which are required for the internet to operate.

The committee recognizes that the executive branch has assigned responsibility for components or sectors of critical infrastructure to various executive branch departments and agencies, and internet architecture is approached in a fractured and piecemeal fashion, with multiple government stakeholder entities claiming responsibility. The committee is concerned that the lack of direction on the subject of internet architecture security creates significant risks to the nation. Consequently, the committee directs the Comptroller General of the United States to provide a report to the House Committee on Armed Services by September 1, 2021, to examine the issue of internet architecture security.

INTELLIGENCE MATTERS

Department of Defense Artificial Intelligence Capabilities and Strategy

The committee believes that global leadership in artificial intelligence (AI) technology is a national security priority. In 2018, the Department of Defense issued a department-wide AI strategy to provide direction for AI development. As the Department increases its investments in AI, machine learning, and other automation technologies, the committee believes that the Department's resources, capabilities, and plans should continue to ensure U.S. competitive advantage over potential adversaries.

Therefore, the committee directs the Comptroller General of the United States to provide the committee with an assessment of the Department's resources, capabilities, and plans for AI. The assessment shall:

(1) describe the Department's overall resource posture, to include personnel and funding, dedicated to AI over the next 5 years;

(2) assess the implementation of the Department's AI strategy, including the extent to which key goals, metrics, and timelines have been developed and attained, and oversight mechanisms have been established, to ensure strategy implementation;

(3) review the functions and missions of the Joint Artificial Intelligence Center, including the actions it is taking to synchronize AI activities across the joint force and the Defense Intelligence Enterprise, including with Project Maven and the Machine-Assisted Analytic Rapid-Repository System;

(4) assess the extent to which the Department has identified key risks that it will face in the increased adoption of AI technologies, and whether it has developed mitigation plans for addressing these risks; and

(5) any other matters the Comptroller General deems appropriate.

The committee further directs the Comptroller General to provide a briefing to the House Committee on Armed Services not later than March 31, 2021, on the Comptroller General's preliminary findings, and to submit a final report to the congressional defense committees on a date agreed to at the time of the briefing.

Joint Intelligence Brigade

The committee notes that obtaining timely intelligence is necessary to support the roles and missions of the Joint Special Operations Command (JSOC) and believes that special operations intelligence components, such as the Joint Intelligence Brigade (JIB), require the appropriate resources and capabilities to support JSOC's strategic direction. As the Department of Defense continues to transition from a primary focus on counterterrorism to focusing on long-term strategic competition and nation-state actors, the committee believes that JSOC and the JIB must ensure that their resources and capabilities also transition to support the priority mission of great power competition.

Therefore, the committee directs the Comptroller General of the United States to provide an assessment of the JIB's resources, functions, and missions. The assessment shall review:

(1) the JIB's resources, to include personnel and funding, over the past 5 years;

(2) the extent to which these resources have increased or decreased over this timeframe;

(3) the functions and missions of the JIB and the extent to which these functions and missions have changed over the past 5 years and are reflective of the current National Security Strategy and JSOC's guidance and direction;

(4) the extent to which the JIB relies on other special operations organizations and the Defense Intelligence Enterprise to meet its functions and missions; and

(5) any other matters the Comptroller General deems appropriate.

The committee further directs the Comptroller General to provide a briefing to the House Committee on Armed Services not later than March 31, 2021, on the Comptroller General's preliminary findings, and to submit a final report to the Committees on Armed Services of the Senate and the House of Representatives on a date agreed to at the time of the briefing.