''(1) Improvements to the source code and documentation for the Ozone Widget Framework.

''(2) Alternative or compatible implementations of the published application programming interface specifications for the Framework.

''(c) ENCOURAGEMENT OF USE AND DEVELOPMENT.—The Chief Information Officer shall, whenever practicable, encourage and foster the use, support, development, and enhancement of the Ozone Widget Framework by the computer industry and commercial information technology vendors, including the development of tools that are compatible with the Framework.''

CONTINUOUS MONITORING OF DEPARTMENT OF DEFENSE INFORMATION SYSTEMS FOR CYBERSECURITY

Pub. L. 111–383, div. A, title IX, § 931, Jan. 7, 2011, 124 Stat. 4334, provided that:

''(a) IN GENERAL.—The Secretary of Defense shall direct the Chief Information Officer of the Department of Defense to work, in coordination with the Chief Information Officers of the military departments and the Defense Agencies and with senior cybersecurity and information assurance officials within the Department of Defense and otherwise within the Federal Government, to achieve, to the extent practicable, the following:

''(1) The continuous prioritization of the policies, principles, standards, and guidelines developed under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3) with agencies and offices operating or exercising control of national security systems (including the National Security Agency) based upon the evolving threat of information security incidents with respect to national security systems, the vulnerability of such systems to such incidents, and the consequences of information security incidents involving such systems.

''(2) The automation of continuous monitoring of the effectiveness of the information security policies, procedures, and practices within the information infrastructure of the Department of Defense, and the compliance of that infrastructure with such policies, procedures, and practices, including automation of—

''(A) management, operational, and technical controls of every information system identified in the inventory required under section 3505(c) of title 44, United States Code; and

''(B) management, operational, and technical controls relied on for evaluations under [former] section 3545 of title 44, United States Code [see now 44 U.S.C. 3555].

''(b) DEFINITIONS.—In this section:

''(1) The term 'information security incident' means an occurrence that—

''(A) actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information such system processes, stores, or transmits; or

''(B) constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies with respect to an information system.

''(2) The term 'information infrastructure' means the underlying framework, equipment, and software that an information system and related assets rely on to process, transmit, receive, or store information electronically.

''(3) The term 'national security system' has the meaning given that term in [former] section 3542(b)(2) of title 44, United States Code [see now 44 U.S.C. 3552(b)(6)].''

§ 2223a. Information technology acquisition planning and oversight requirements

(a) ESTABLISHMENT OF PROGRAM.—The Secretary of Defense shall establish a program to improve the planning and oversight processes for the acquisition of major automated information systems by the Department of Defense.

(b) PROGRAM COMPONENTS.—The program established under subsection (a) shall include—

(1) a documented process for information technology acquisition planning, requirements development and management, project management and oversight, earned value management, and risk management;

(2) the development of appropriate metrics that can be implemented and monitored on a real-time basis for performance measurement of—

(A) processes and development status of investments in major automated information system programs;

(B) continuous process improvement of such programs; and

(C) achievement of program and investment outcomes;

(3) a process to ensure that key program personnel have an appropriate level of experience, training, and education in the planning, acquisition, execution, management, and oversight of information technology systems;

(4) a process to ensure sufficient resources and infrastructure capacity for test and evaluation of information technology systems;

(5) a process to ensure that military departments and Defense Agencies adhere to established processes and requirements relating to the planning, acquisition, execution, management, and oversight of information technology programs and developments; and

(6) a process under which an appropriate Department of Defense official may intervene or terminate the funding of an information technology investment if the investment is at risk of not achieving major project milestones.

(Added Pub. L. 111–383, div. A, title VIII, § 805(a)(1), Jan. 7, 2011, 124 Stat. 4259.)

ESTABLISHMENT OF SECURE NEXT-GENERATION WIRELESS NETWORK (5G) INFRASTRUCTURE FOR THE NEVADA TEST AND TRAINING RANGE AND BASE INFRASTRUCTURE

Pub. L. 116–92, div. A, title II, § 226, Dec. 20, 2019, 133 Stat. 1269, provided that:

''(a) ESTABLISHMENT REQUIRED.—Not later than one year after the date of the enactment of this Act [Dec. 20, 2019], the Secretary of Defense shall establish secure fifth-generation wireless network components and capabilities at no fewer than two Department of Defense installations in accordance with this section.

''(b) INSTALLATIONS.—

''(1) LOCATIONS.—The Secretary shall establish components and capabilities under subsection (a) at the following:

''(A) The Nevada Test and Training Range, which shall serve as a Major Range and Test Facility Base (MRTFB) for fifth-generation wireless networking.

''(B) Such Department installations or other installations as the Secretary considers appropriate for the purpose set forth in paragraph (2).

''(2) PURPOSE.—The purpose of the establishment of components and capabilities under subsection (a) at the locations described in paragraph (1) of this subsection is to demonstrate the following:

''(A) The potential military utility of high bandwidth, scalable, and low latency fifth-generation wireless networking technology.

''(B) Advanced security technology that is applicable to fifth-generation networks as well as legacy Department command and control networks.

''(C) Secure interoperability with fixed and wireless systems (legacy and future systems).

''(D) Enhancements such as spectrum and waveform diversity, frequency hopping and spreading, and beam forming for military requirements.

''(E) Technology for dynamic network slicing for specific use cases and applications requiring varying levels of latency, scale, and throughput.

''(F) Technology for dynamic spectrum sharing and network isolation.

''(G) Base infrastructure installation of high bandwidth, scalable, and low latency fifth-generation wireless networking technology.

''(H) Applications for secure fifth-generation wireless network capabilities for the Department, such as the following:

''(i) Interactive augmented reality or synthetic training environments.

''(ii) Internet of things devices.

''(iii) Autonomous systems.

''(iv) Advanced manufacturing through the following:

''(I) Department-sponsored centers for manufacturing innovation (as defined in section 34(c) of the National Institute of Standards and Technology Act (15 U.S.C. 278s(c))).

''(II) Department research and development organizations.

''(III) Manufacturers in the defense industrial base of the United States.''

DIGITAL ENGINEERING CAPABILITY TO AUTOMATE TESTING AND EVALUATION

Pub. L. 116–92, div. A, title II, § 231, Dec. 20, 2019, 133 Stat. 1274, provided that:

''(a) DIGITAL ENGINEERING CAPABILITY.—

''(1) IN GENERAL.—The Secretary of Defense shall establish a digital engineering capability to be used—

''(A) for the development and deployment of digital engineering models for use in the defense acquisition process; and

''(B) to provide testing infrastructure and software to support automated approaches for testing, evaluation, and deployment throughout the defense acquisition process.

''(2) REQUIREMENTS.—The capability developed under subsection (a) shall meet the following requirements:

''(A) The capability will be accessible to, and useable by, individuals throughout the Department of Defense who have responsibilities relating to capability design, development, testing, evaluation, and operation.

''(B) The capability will provide for the development, validation, use, curation, and maintenance of technically accurate digital systems, models of systems, subsystems, and their components, at the appropriate level of fidelity to ensure that test activities adequately simulate the environment in which a system will be deployed.

''(C) The capability will include software to automate testing throughout the program life cycle, including to satisfy developmental test requirements and operational test requirements. Such software may be developed in accordance with the authorities provided under section 800 [of Pub. L. 116–92, set out as a note below], and shall support—

''(i) security testing that includes vulnerability scanning and penetration testing performed by individuals, including threat-based red team exploitations and assessments with zero-trust assumptions; and

''(ii) high-confidence distribution of software to the field on a time-bound, repeatable, frequent, and iterative basis.

''(b) DEMONSTRATION ACTIVITIES.—

''(1) IN GENERAL.—In developing the capability required under subsection (a), the Secretary of Defense shall carry out activities to demonstrate digital engineering approaches to automated testing that—

''(A) enable continuous software development and delivery;

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

''(C) satisfy operational test and evaluation requirements for such programs.

''(2) PROGRAM SELECTION.—Not later than 180 days after the date of the enactment of this Act [Dec. 20, 2019], the Secretary of Defense shall assess and select not fewer than four and not more than ten programs of the Department of Defense to participate in the demonstration activities under paragraph (1), including—

''(A) at least one program participating in the pilot program authorized under section 873 of the National Defense Authorization Act for Fiscal Year 2018 (Public Law 115–91; 10 U.S.C. 2223a note);

''(B) at least one program participating in the pilot program authorized under section 874 of such Act (Public Law 115–91; 10 U.S.C. 2302 note);

''(C) at least one major defense acquisition program (as defined in section 2430 of title 10, United States Code);

''(D) at least one command and control program;

''(E) at least one defense business system (as defined in section 2222(i) of title 10, United States Code); and

''(F) at least one program from each military service.

''(3) ADDITIONAL REQUIREMENTS.—As part of the demonstration activities under paragraph (1), the Secretary shall—

''(A) conduct a comparative analysis that assesses the risks and benefits of the digital engineering supported automated testing approaches of the programs participating in the demonstration activities relative to traditional testing approaches that are not supported by digital engineering;

''(B) ensure that the intellectual property strategy for each of the programs participating in the demonstration activities is best aligned to meet the goals of the program; and

''(C) develop a workforce and infrastructure plan to support any new policies and guidance implemented in connection with the demonstration activities, including any policies and guidance implemented after the completion of such activities.

''(c) POLICIES AND GUIDANCE REQUIRED.—Not later than one year after the date of the enactment of this Act [Dec. 20, 2019], based on the results of the demonstration activities carried out under subsection (b), the Secretary of Defense shall issue or modify policies and guidance to—

''(1) promote the use of digital engineering capabilities for development and for automated testing; and

''(2) address roles, responsibilities, and procedures relating to such capabilities.

''(d) STEERING COMMITTEE.—

''(1) IN GENERAL.—The Secretary of Defense shall establish a steering committee to assist the Secretary in carrying out subsections (a) through (c).

''(2) MEMBERSHIP.—The steering committee shall be composed of the following members or their designees:

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

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

''(C) The Chief Information Officer.

''(D) The Director of Operational Test and Evaluation.

''(E) The Director of Cost Assessment and Program Evaluation.

''(F) The Service Acquisition Executives.

''(G) The Service testing commands.

''(H) The Director of the Defense Digital Service.

''(e) REPORTS REQUIRED.—

''(1) IMPLEMENTATION.—Not later than March 15, 2020, the Secretary of Defense shall submit to the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and

the House of Representatives] a report on the progress of the Secretary in implementing subsections (a) through (c). The report shall include an explanation of how the results of the demonstration activities carried out under subsection (b) will be incorporated into the policy and guidance required under subsection (c), particularly the policy and guidance of the members of the steering committee established under subsection (d).

''(2) LEGISLATIVE RECOMMENDATIONS.—Not later than October 15, 2020, the Secretary of Defense shall provide to the congressional defense committees a briefing that identifies any changes to existing law that may be necessary to facilitate the implementation of subsections (a) through (c).

''(f) INDEPENDENT ASSESSMENT.—

''(1) IN GENERAL.—Not later than March 15, 2021, the Defense Innovation Board and the Defense Science Board shall jointly complete an independent assessment of the progress of the Secretary in implementing subsections (a) through (c). The Secretary of Defense shall ensure that the Defense Innovation Board and the Defense Science Board have access to the resources, data, and information necessary to complete the assessment.

''(2) INFORMATION TO CONGRESS.—Not later than 30 days after the date on which the assessment under paragraph (1) is completed, the Defense Innovation Board and the Defense Science Board shall jointly provide to the congressional defense committees—

''(A) a report summarizing the assessment; and

''(B) a briefing on the findings of the assessment.''

STRATEGY AND IMPLEMENTATION PLAN FOR FIFTH GENERATION INFORMATION AND COMMUNICATIONS TECHNOLOGIES

Pub. L. 116–92, div. A, title II, § 254, Dec. 20, 2019, 133 Stat. 1287, provided that:

''(a) IN GENERAL.—Not later than 270 days after the date of the enactment of this Act [Dec. 20, 2019], the Secretary of Defense shall develop—

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

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

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

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

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

''(A) 5G testbeds for developing military and dual-use applications; and

''(B) spectrum-sharing technologies and frameworks.

''(3) Strengthening engagement and outreach with industry, academia, international partners, and other departments and agencies of the Federal Government on issues relating to 5G technology and the deployment of such technology, including development of a common industrial base for secure microelectronics.

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

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

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

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

''(8) Advancing the deployment of secure 5G networks nationwide.

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

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

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

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

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

''(4) The Under Secretary of Defense for Intelligence [now Under Secretary of Defense for Intelligence and Security].

''(5) Service Acquisition Executives of each military service.

''(d) PERIODIC BRIEFINGS.—

''(1) IN GENERAL.—Not later than March 15, 2020, and not less frequently than once every three months thereafter through March 15, 2022, the Secretary of Defense shall provide to the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] a briefing on the development and implementation of the strategy required under subsection (a), including an explanation of how the Department of Defense—

''(A) is using secure 5G wireless network technology;

''(B) is reshaping the Department's policy for producing and procuring secure microelectronics; and

''(C) is working in the interagency and internationally to develop common policies and approaches.

''(2) ELEMENTS.—Each briefing under paragraph (1) shall include information on—

''(A) efforts to ensure a secure supply chain for 5G wireless network equipment and microelectronics;

''(B) the continued availability of electromagnetic spectrum for warfighting needs;

''(C) planned implementation of 5G wireless network infrastructure in warfighting networks, base infrastructure, defense-related manufacturing, and logistics;

''(D) steps taken to work with allied and partner countries to protect critical networks and supply chains; and

''(E) such other topics as the Secretary of Defense considers relevant.''

DEPARTMENT-WIDE SOFTWARE SCIENCE AND TECHNOLOGY STRATEGY

Pub. L. 116–92, div. A, title II, § 255, Dec. 20, 2019, 133 Stat. 1288, provided that:

''(a) DESIGNATION OF SENIOR OFFICIAL.—Not later than 180 days after the date of the enactment of this Act [Dec. 20, 2019], the Secretary of Defense, acting through the Under Secretary of Defense for Research and Engineering and in consultation with the Under Secretary of Defense for Acquisition and Sustainment and appropriate public and private sector organizations, shall designate a single official or existing entity within the Department of Defense as the official or entity (as the case may be) with principal responsibility for guiding the development of science and technology activities related to next generation software and software reliant systems for the Department, including—

''(1) research and development activities on new technologies for the creation of highly secure, scalable, reliable, time-sensitive, and mission-critical software;

''(2) research and development activities on new approaches and tools to software development and deployment, testing, integration, and next generation software management tools to support the rapid insertion of such software into defense systems;

''(3) foundational scientific research activities to support advances in software;

''(4) technical workforce and infrastructure to support defense science and technology and software needs and mission requirements;

''(5) providing capabilities, including technologies, systems, and technical expertise to support improved acquisition of software reliant business and warfighting systems; and

''(6) providing capabilities, including technologies, systems, and technical expertise to support defense operational missions which are reliant on software.

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

''(1) types of software-related activities within the science and technology portfolio of the Department;

''(2) investment in new approaches to software development and deployment, and next generation management tools;

''(3) ongoing research and other support of academic, commercial, and development community efforts to innovate the software development, engineering, and testing process, automated testing, assurance and certification for safety and mission critical systems, large scale deployment, and sustainment;

''(4) to the extent practicable, implementing or continuing the implementation of the recommendations set forth in—

''(A) the final report of the Defense Innovation Board submitted to the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] under section 872 of the National Defense Authorization Act for Fiscal Year 2018 (Public Law 115–91; 131 Stat. 1497);

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

''(C) other relevant studies on software research, development, and acquisition activities of the Department of Defense.

''(5) supporting the acquisition, technology development, testing, assurance, and certification and operational needs of the Department through the development of capabilities, including personnel and research and production infrastructure, and programs in—

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

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

''(C) the Defense Advanced Research Projects Agency; and

''(D) universities, federally funded research and development centers, and service organizations with activities in software engineering; and

''(6) the transition of relevant capabilities and technologies to relevant programs of the Department, including software-reliant cyber-physical systems, tactical systems, enterprise systems, and business systems.

''(c) SUBMITTAL TO CONGRESS.—Not later than one year after the date of the enactment of this Act [Dec. 20, 2019], the official or entity designated under subsection (a) shall submit to the congressional defense committees the strategy developed under subsection (b).''

AUTHORITY FOR CONTINUOUS INTEGRATION AND DELIVERY OF SOFTWARE APPLICATIONS AND UPGRADES TO EMBEDDED SYSTEMS

Pub. L. 116–92, div. A, title VIII, § 800, Dec. 20, 2019, 133 Stat. 1478, provided that:

''(a) SOFTWARE ACQUISITION AND DEVELOPMENT PATHWAYS.—The Secretary of Defense shall establish pathways as described under subsection (b) to provide for the efficient and effective acquisition, development, integration, and timely delivery of secure software. Such a pathway shall include the following:

''(1) USE OF PROVEN TECHNOLOGIES AND SOLUTIONS.—A pathway established under this section shall provide for the use of proven technologies and solutions to continuously engineer and deliver capabilities in software.

''(2) USE OF AUTHORITY.—In using the authority under this section, the Secretary shall consider how such use will—

''(A) initiate the engineering of new software capabilities quickly;

''(B) demonstrate the viability and effectiveness of such capabilities for operational use not later than one year after the date on which funds are first obligated to acquire or develop software; and

''(C) allow for the continuous updating and delivery of new capabilities not less frequently than annually to iteratively meet a requirement.

''(3) TREATMENT NOT AS MAJOR DEFENSE ACQUISITION PROGRAM.—Software acquired or developed using the authority under this section shall not be treated as a major defense acquisition program for purposes of section 2430 of title 10, United States Code, or Department of Defense Directive 5000.01 without the specific direction of the Under Secretary of Defense for Acquisition and Sustainment or a Senior Acquisition Executive.

''(4) RISK-BASED APPROACH.—The Secretary of Defense shall use a risk-based approach for the consideration of innovative technologies and new capabilities for software to be acquired or developed under this authority to meet needs communicated by the Joint Chiefs of Staff and the combatant commanders.

''(b) PATHWAYS.—The Secretary of Defense may establish as many pathways as the Secretary determines appropriate and shall establish the following pathways:

''(1) APPLICATIONS.—The applications software acquisition pathway shall provide for the use of rapid development and implementation of applications and other software or software improvements operated by the Department of Defense, which may include applications running on commercial commodity hardware (including modified hardware) and commercially available cloud computing platforms.

''(2) EMBEDDED SYSTEMS.—The embedded systems software acquisition pathway shall provide for the rapid development and insertion of upgrades and improvements for software embedded in weapon systems and other military-unique hardware systems.

''(c) EXPEDITED PROCESS.—

''(1) IN GENERAL.—A pathway established under subsection (a) shall provide for—

''(A) a streamlined and coordinated requirements, budget, and acquisition process to support rapid fielding of software applications and of software upgrades to embedded systems for operational use in a period of not more than one year from the time that the process is initiated;

''(B) the collection of data on software fielded; and

''(C) continuous engagement with the users of software to support engineering activities, and to support delivery of software for operational use in periods of not more than one year.

''(2) EXPEDITED SOFTWARE REQUIREMENTS PROCESS.—

''(A) INAPPLICABILITY OF JOINT CAPABILITIES INTEGRATION AND DEVELOPMENT SYSTEM (JCIDS) MANUAL.—Software acquisition or development conducted under the authority of this section shall not be subject to the Joint Capabilities Integration and Development System Manual, except pursuant to a modified process specifically provided for the acquisition or development of software by the Vice Chairman of the Joint Chiefs of Staff, in consultation with Under Secretary of Defense for Acquisi-

tion and Sustainment and each service acquisition executive (as defined in section 101(a)(10) of title 10, United States Code).

''(B) INAPPLICABILITY OF DEFENSE ACQUISITION SYSTEM DIRECTIVE.—Software acquisition or development conducted under the authority of this section shall not be subject to Department of Defense Directive 5000.01, except when specifically provided for the acquisition or development of software by the Under Secretary of Defense for Acquisition and Sustainment, in consultation with the Vice Chairman of the Joint Chiefs of Staff and each service acquisition executive.

''(d) ELEMENTS.—In implementing a pathway established under the authority of this section, the Secretary shall tailor requirements relating to—

''(1) iterative development of requirements for software to be acquired or developed under the authority of this section through engagement with the user community and through the use of operational user feedback, in order to continuously define and update priorities for such requirements;

''(2) early identification of the warfighter or user need, including the rationale for how software capabilities will support increased lethality and efficiency, and identification of a relevant user community;

''(3) initial contract requirements and format, including the use of summary-level lists of problems and shortcomings in existing software and desired features or capabilities of new or upgraded software;

''(4) continuous refinement and prioritization of contract requirements through use of evolutionary processes, informed by continuous engagement with operational users throughout the development and implementation period;

''(5) continuous consideration of issues related to lifecycle costs, technical data rights, and systems interoperability;

''(6) planning for support of software capabilities in cases where the software developer may stop supporting the software;

''(7) rapid contracting procedures, including expedited timeframes for making awards, selecting contract types, defining teaming arrangements, and defining options;

''(8) program execution processes, including supporting development and test infrastructure, automation and tools, digital engineering, data collection and sharing with Department of Defense oversight organizations and with Congress, the role of developmental and operational testing activities, key decision making and oversight events, and supporting processes and activities (such as independent costing activity, operational demonstration, and performance metrics);

''(9) assurances that cybersecurity metrics of the software to be acquired or developed, such as metrics relating to the density of vulnerabilities within the code of such software, the time from vulnerability identification to patch availability, the existence of common weaknesses within such code, and other cybersecurity metrics based on widely-recognized standards and industry best practices, are generated and made available to the Department of Defense and the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives];

''(10) administrative procedures, including procedures related to who may initiate and approve an acquisition under this authority, the roles and responsibilities of the implementing project or product teams and supporting activities, team selection and staffing process, governance and oversight roles and responsibilities, and appropriate independent technology assessments, testing, and cost estimation (including relevant thresholds or designation criteria);

''(11) mechanisms and waivers designed to ensure flexibility in the implementation of a pathway under this section, including the use of other transaction authority, broad agency announcements, and other procedures; and

''(12) mechanisms the Secretary will use for appropriate reporting to Congress on the use of this authority, including notice of initiation of the use of a pathway and data regarding individual programs or acquisition activities, how acquisition activities are reflected in budget justification materials or requests to reprogram appropriated funds, and compliance with other reporting requirements.

''(e) GUIDANCE REQUIRED.—

''(1) IN GENERAL.—Not later than 90 days after the date of the enactment of this Act [Dec. 20, 2019], the Secretary of Defense shall issue initial guidance to implement the requirements of this section.

''(2) LIMITATION.—If the Secretary of Defense has not issued final guidance to implement the requirements of this section before October 1, 2021, the Secretary may not use the authority under this section—

''(A) to establish a new pathway to acquire or develop software; or

''(B) to continue activities to acquire or develop software using a pathway established under initial guidance described in paragraph (1).

''(f) REPORT.—

''(1) IN GENERAL.—Not later than October 15, 2020, the Under Secretary of Defense for Acquisition and Sustainment, in consultation with the secretaries of the military departments and other appropriate officials, shall report on the use of the authority under this section using the initial guidance issued under subsection (d).

''(2) ELEMENTS.—The report required under paragraph (1) shall include the following elements:

''(A) The final guidance required by subsection (d)(2), including a description of the treatment of use of the authority that was initiated before such final guidance was issued.

''(B) A summary of how the authority under this section has been used, including a list of the cost estimate, schedule for development, testing and delivery, and key management risks for each initiative conducted pursuant to such authority.

''(C) Accomplishments from and challenges to using the authority under this section, including organizational, cultural, talent, infrastructure, testing, and training considerations.

''(D) Recommendations for legislative changes to the authority under this section.

''(E) Recommendations for regulatory changes to the authority under this section to promote effective development and deployment of software acquired or developed under this section.''

REORIENTATION OF BIG DATA PLATFORM PROGRAM

Pub. L. 116–92, div. A, title XVI, §1651, Dec. 20, 2019, 133 Stat. 1759, provided that:

''(a) REORIENTATION OF PROGRAM.—

''(1) IN GENERAL.—Not later than January 1, 2021, the Secretary of Defense shall—

''(A) reorient the Big Data Platform program as specified in this section; and

''(B) align the reorientation effort under an existing line of effort of the Cyber Strategy of the Department of Defense.

''(2) OVERSIGHT OF IMPLEMENTATION.—The Secretary shall act through the Principal Cyber Advisor and the supporting Cross Functional Team in the oversight of the implementation of paragraph (1).

''(b) COMMON BASELINE AND SECURITY CLASSIFICATION SCHEME.—

''(1) IN GENERAL.—Not later than January 1, 2021, the Secretary shall establish a common baseline and security classification scheme for the collection, storage, processing, querying, analysis, and accessibility of a common and comprehensive set of metadata from sensors, applications, appliances, products, and systems deployed across the Department of Defense Information Network (DODIN) to enable the discovery, tracking, and remediation of cybersecurity threats.

''(2) REQUIREMENTS.—In carrying out paragraph (1), the Secretary shall—

''(A) take such actions as the Secretary considers necessary to standardize deployed infrastructure, including the Department of Defense's perimeter capabilities at the Internet Access Points, the Joint Regional Security Stacks, or other approved solutions, and the routing of data laterally and vertically from Department of Defense Information Network segments and tiers, to enable standard and comprehensive metadata collection;

''(B) take such actions as the Secretary considers necessary to standardize deployed cybersecurity applications, products, and sensors and the routing of data laterally and vertically from Department of Defense Information Network segments and tiers, to enable standard and comprehensive metadata collection;

''(C) develop an enterprise-wide architecture and strategy for—

''(i) where to place sensors or extract data from network information technology, operational technology, and cybersecurity appliances, applications, products, and systems for cybersecurity purposes;

''(ii) which metadata data records should be universally sent to Big Data Platform instances and which metadata data records, if any, should be locally retained; and

''(iii) expeditiously and efficiently transmitting metadata records to the Big Data Platform instances, including the acquisition and installation of further data bandwidth;

''(D) determine the appropriate number, organization, and functions of separate Big Data Platform instances, and whether the Big Data Platform instances that are currently managed by Department of Defense components, including the military services, should instead be jointly and regionally organized, or terminated;

''(E) determine the appropriate roles of the Defense Information Systems Agency's Acropolis, United States Cyber Command's Scarif, and any similar Big Data Platforms as enterprise-wide real-time cybersecurity situational awareness capabilities or as complements or replacements for component level Big Data Platform instances;

''(F) ensure that all Big Data Platform instances are engineered and approved to enable standard access and expeditious query capabilities by the Unified Platform, the network defense service providers, and the Cyber Mission Forces, with centrally managed authentication and authorization services;

''(G) prohibit and remove barriers to information sharing, distributed query, data analysis, and collaboration across Big Data Platform instances, such as incompatible interfaces, interconnection service agreements, and the imposition of accreditation boundaries;

''(H) transition all Big Data Platform instances to a cloud computing environment in alignment with the cloud strategy of the Chief Information Officer of the Department of Defense;

''(I) consider whether packet capture databases should continue to be maintained separately from the Big Data Platform instances, managed at the secret level of classification, and treated as malware-infected when the packet data are copies of packets extant in the Department of Defense Information Network;

''(J) in the case that the Secretary decides to sustain the status quo on packet capture databases, ensure that analysts operating on or from the Unified Platform, the Big Data Platform instances, the network defense services providers, and the Cyber Mission Forces can directly access packets and query the database; and

''(K) consider whether the Joint Artificial Intelligence Center's cybersecurity artificial intelligence national mission initiative, and any other similar initiatives, should include an application for the metadata residing in the Big Data Platform instances.

''(c) LIMIT ON DATA AND DATA INDEXING SCHEMA.—The Secretary shall ensure that the Unified Platform and the Big Data Platform programs achieve data and data indexing schema standardization and integration to ensure interoperability, access, and sharing by and between Big Data Platform and other data sources and stores.

''(d) ANALYTICS AND APPLICATION SOURCING AND COLLABORATION.—The Secretary shall ensure that the services, U.S. Cyber Command, and Defense Information Systems Agency—

''(1) seek advanced analytics and applications from Government and commercial sources that can be executed on the deployed Big Data Platform architecture; and

''(2) collaborate with vendors offering commercial analytics and applications, including support to refactoring commercial capabilities to the Government platform where industry can still own the intellectual property embedded in the analytics and applications.

''(e) BRIEFING REQUIRED.—Not later than 180 days after the date of the enactment of this Act [Dec. 20, 2019] and not less frequently than once every 180 days thereafter until the activities required by subsection (a)(1) are completed, the Secretary shall brief the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] on the activities of the Secretary in carrying out subsection (b).''

POLICY REGARDING THE TRANSITION OF DATA AND APPLICATIONS TO THE CLOUD

Pub. L. 116–92, div. A, title XVII, §1755, Dec. 20, 2019, 133 Stat. 1854, provided that:

''(a) POLICY REQUIRED.—Not later than 180 days after the date of the enactment of this Act [Dec. 20, 2019], the Chief Information Officer of the Department of Defense and the Chief Data Officer of the Department shall, in consultation with the J6 of the Joint Staff and the Chief Management Officer, develop and issue enterprise-wide policy and implementing instructions regarding the transition of data and applications to the cloud under the Department cloud strategy in accordance with subsection (b).

''(b) DESIGN.—The policy required by subsection (a) shall be designed to dramatically improve support to operational missions and management processes, including by the use of artificial intelligence and machine learning technologies, by—

''(1) making the data of the Department available to support new types of analyses;

''(2) preventing, to the maximum extent practicable, the replication in the cloud of data stores that cannot readily be accessed by applications for which the data stores were not originally engineered;

''(3) ensuring that data sets can be readily discovered and combined with others to enable new insights and capabilities; and

''(4) ensuring that data and applications are readily portable and not tightly coupled to a specific cloud infrastructure or platform.''

IMPLEMENTATION OF RECOMMENDATIONS OF THE FINAL REPORT OF THE DEFENSE SCIENCE BOARD TASK FORCE ON THE DESIGN AND ACQUISITION OF SOFTWARE FOR DEFENSE SYSTEMS

Pub. L. 115–232, div. A, title VIII, §868, Aug. 13, 2018, 132 Stat. 1902, provided that:

''(a) IMPLEMENTATION REQUIRED.—Not later than 18 months after the date of the enactment of this Act [Aug. 13, 2018], the Secretary of Defense shall, except as provided under subsection (b), commence implementation of each recommendation submitted as part of the final report of the Defense Science Board Task Force

on the Design and Acquisition of Software for Defense Systems.

''(b) EXCEPTIONS.—

''(1) DELAYED IMPLEMENTATION.—The Secretary of Defense may commence implementation of a recommendation described under subsection (a) later than the date required under such subsection if the Secretary provides the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] with a specific justification for the delay in implementation of such recommendation.

''(2) NONIMPLEMENTATION.—The Secretary of Defense may opt not to implement a recommendation described under subsection (a) if the Secretary provides to the congressional defense committees—

''(A) the reasons for the decision not to implement the recommendation; and

''(B) a summary of the alternative actions the Secretary plans to take to address the purposes underlying the recommendation.

''(c) IMPLEMENTATION PLANS.—For each recommendation that the Secretary is implementing, or that the Secretary plans to implement, the Secretary shall submit to the congressional defense committees—

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

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

ACTIVITIES AND REPORTING RELATING TO DEPARTMENT OF DEFENSE'S CLOUD INITIATIVE

Pub. L. 115–232, div. A, title X, § 1064, Aug. 13, 2018, 132 Stat. 1971, provided that:

''(a) ACTIVITIES REQUIRED.—Commencing not later than 90 days after the date of the enactment of this Act [Aug. 13, 2018], the Chief Information Officer of the Department of Defense, acting through the Cloud Executive Steering Group established by the Deputy Secretary of Defense in a directive memorandum dated September 13, 2017, in order to support its Joint Enterprise Defense Infrastructure initiative to procure commercial cloud services, shall conduct certain key enabling activities as follows:

''(1) Develop an approach to rapidly acquire advanced commercial network capabilities, including software-defined networking, on-demand bandwidth, and aggregated cloud access gateways, through commercial service providers in order—

''(A) to support the migration of applications and systems to commercial cloud platforms;

''(B) to increase visibility of end-to-end performance to enable and enforce service level agreements for cloud services;

''(C) to ensure efficient and common cloud access;

''(D) to facilitate shifting data and applications from one cloud platform to another;

''(E) to improve cybersecurity; and

''(F) to consolidate networks and achieve efficiencies and improved performance;

''(2) Conduct an analysis of existing workloads that would be migrated to the Joint Enterprise Defense Infrastructure, including—

''(A) identifying all of the cloud initiatives across the Department of Defense, and determining the objectives of such initiatives in connection with the intended scope of the Infrastructure;

''(B) identifying all the systems and applications that the Department would intend to migrate to the Infrastructure;

''(C) conducting rationalization of applications to identify applications and systems that may duplicate the processing of workloads in connection with the Infrastructure; and

''(D) as result of such actions, arriving at dispositions about migration or termination of systems and applications in connection with the Infrastructure.

''(b) REPORT REQUIRED.—The Chief Information Officer shall submit to the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] a report on the Department of Defense's Cloud Initiative to manage networks, data centers, and clouds at the enterprise level. Such report shall include each of the following:

''(1) A description [of] the status of completion of the activities required under subsection (a).

''(2) Information relating to the current composition of the Cloud Executive Steering Group and the stakeholders relating to the Department of Defense's Cloud Initiative and associated mission, objectives, goals, and strategy.

''(3) A description of the characteristics and considerations for accelerating the cloud architecture and services required for a global, resilient, and secure information environment.

''(4) Information relating to acquisition strategies and timeline for efforts associated with the Department of Defense's Cloud Initiative, including the Joint Enterprise Defense Infrastructure.

''(5) A description of how the acquisition strategies referred to in paragraph (4) provides [sic] for a full and open competition, enable the Department of Defense to continuously leverage and acquire new cloud computing capabilities, maintain the ability of the Department to leverage other cloud computing vendor products and services, incorporate elements to maintain security, and provide for the best performance, cost, and schedule to meet the cloud architecture and services requirements of the Department for the duration of such contract.

''(6) A detailed description of existing workloads that will be migrated to enterprise-wide cloud infrastructure or platforms as a result of the Department of Defense's Cloud Initiative, including estimated migration costs and timelines, based on the analysis required under subsection (a)(2).

''(7) A description of the program management and program office of the Department of Defense's Cloud Initiative, including the number of personnel, overhead costs, and organizational structure.

''(8) A description of the effect of the Joint Enterprise Defense Infrastructure on and the relationship of such Infrastructure to existing cloud computing infrastructure, platform, and service contracts across the Department of Defense, specifically the effect and relationship to the private cloud infrastructure of the Department, MilCloud 2.0 run by the Defense Information Systems Agency based on the analysis required under subsection (a)(2).

''(9) Information relating to the most recent Department of Defense Cloud Computing Strategy and description of any initiatives to update such Strategy.

''(10) Information relating to Department of Defense guidance pertaining to cloud computing capability or platform acquisition and standards, and a description of any initiatives to update such guidance.

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

''(c) LIMITATION ON USE OF FUNDS.—Of the amounts authorized to be appropriated or otherwise made available by this Act [see Tables for classification] for fiscal year 2019 for the Department of Defense's Cloud Initiative, not more than 85 percent may be obligated or expended until the Secretary of Defense submits to the congressional defense committees the report required by subsection (b).

''(d) LIMITATION ON NEW SYSTEMS AND APPLICATIONS.—

''(1) IN GENERAL.—Except as provided in paragraph (2), the Deputy Secretary shall require that no new system or application will be approved for development or modernization without an assessment that such system or application is already, or can and would be, cloud-hosted.

''(2) WAIVER.—The Deputy Secretary may issue a national waiver to the requirement under paragraph

(1) if the Deputy Secretary determines, pursuant to the assessment described in such paragraph, that the requirement would adversely affect the national security of the United States. If the Deputy Secretary issues a waiver under this paragraph, the Deputy Secretary shall provide to the congressional defense committees a written notification of such waiver, justification for the waiver, and identification of the system or application to which the waiver applies by not later than 15 days after the date on which the waiver is issued.

''(e) TRANSPARENCY AND COMPETITION.—The Deputy Secretary shall ensure that the acquisition approach of the Department continues to follow the Federal Acquisition Regulation with respect to competition.''

PILOT PROGRAM TO USE AGILE OR ITERATIVE DEVELOPMENT METHODS TO TAILOR MAJOR SOFTWARE-INTENSIVE WARFIGHTING SYSTEMS AND DEFENSE BUSINESS SYSTEMS

Pub. L. 115–232, div. A, title VIII, §869(a)–(d), Aug. 13, 2018, 132 Stat. 1902, 1903, provided that:

''(a) IN GENERAL.—Not later than 30 days after the date of the enactment of this Act [Aug. 13, 2018], the Secretary of Defense shall include the following systems in the pilot program to use agile or iterative development methods pursuant to section 873 of the National Defense Authorization Act for Fiscal Year 2018 (Public Law 115–91; 10 U.S.C. 2223a note):

''(1) Defense Retired and Annuitant Pay System 2 (DRAS2), Defense Logistics Agency.

''(2) Army Integrated Air and Missile Defense (AIAMD), Army.

''(3) Army Contract Writing System (ACWS), Army.

''(4) Defense Enterprise Accounting and Management System (DEAMS) Inc2, Air Force.

''(5) Item Master, Air Force.

''(b) ADDITIONS TO LIST.—Not later than 30 days after the date of the enactment of this Act, the Secretary of Defense shall identify three additional systems for participation in the pilot program pursuant to section 873 of the National Defense Authorization Act for Fiscal Year 2018 (Public Law 115–91; 10 U.S.C. 2223a note) and notify the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] of the additions.

''(c) COMMUNITY OF PRACTICE ADVISING ON AGILE OR ITERATIVE DEVELOPMENT.—The Under Secretary of Defense for Acquisition and Sustainment shall establish a Community of Practice on agile or iterative methods so that programs that have been incorporating agile or iterative methods can share with programs participating in the pilot the lessons learned, best practices, and recommendations for improvements to acquisition and supporting processes. The Service Acquisition Executives of the military departments shall send representation from the following programs, which have reported using agile or iterative methods:

''(1) Air and Space Operations Center (AOC).

''(2) Command Control Battle Management and Communications (C2BMC).

''(3) The family of Distributed Common Ground Systems.

''(4) The family of Global Command and Control Systems.

''(5) Navy Personnel and Pay (NP2).

''(6) Other programs and activities as appropriate.

''(d) REPORT.—Not later than 180 days after the date of the enactment of this Act, the Secretary of Defense shall report to the congressional defense committees on the status of the pilot program and each system participating in the pilot. The report shall include the following elements:

''(1) A description of how cost and schedule estimates in support of the program are being conducted and using what methods.

''(2) The contracting strategy and types of contracts that will be used in executing the program.

''(3) A description of how intellectual property ownership issues associated with software applications developed with agile or iterative methods will be addressed to ensure future sustainment, maintenance, and upgrades to software applications after the applications are fielded.

''(4) A description of the tools and software applications that are expected to be developed for the program and the costs and cost categories associated with each.

''(5) A description of challenges the program has faced in realigning the program to use agile or iterative methods.''

Pub. L. 115–91, div. A, title VIII, §873, Dec. 12, 2017, 131 Stat. 1498, as amended by Pub. L. 115–232, div. A, title VIII, §869(e), Aug. 13, 2018, 132 Stat. 1903, provided that:

''(a) PILOT PROGRAM.—

''(1) IN GENERAL.—Not later than 30 days after the date of the enactment of this Act [Dec. 12, 2017], the Secretary of Defense, in consultation with the Secretaries of the military departments and the chiefs of the armed forces, shall establish a pilot program to tailor and simplify software development requirements and methods for major software-intensive warfighting systems and defense business systems.

''(2) IMPLEMENTATION PLAN FOR PILOT PROGRAM.—Not later than 120 days after the date of the enactment of this Act, the Secretary of Defense, in consultation with the Secretaries of the military departments and the chiefs of the armed forces, shall develop a plan for implementing the pilot program required under this subsection, including guidance for implementing the program and for selecting systems for participation in the program.

''(3) SELECTION OF SYSTEMS FOR PILOT PROGRAM.—

''(A) The implementation plan shall require that systems be selected as follows:

''(i) For major software-intensive warfighting systems, one system per armed force and one defense-wide system, including at least one major defense acquisition program or major automated information system.

''(ii) For defense business systems, not fewer than two systems and not greater than eight systems.

''(B) In selecting systems or subsystems for participation, the Secretary shall prioritize systems as follows:

''(i) For major software-intensive warfighting systems, systems that—

''(I) have identified software development as a high risk;

''(II) have experienced cost growth and schedule delay; or

''(III) did not deliver any operational capability within the prior calendar year.

''(ii) For defense business systems, systems that—

''(I) have experienced cost growth and schedule delay;

''(II) did not deliver any operational capability within the prior calendar year; or

''(III) are underperforming other systems within a defense business system portfolio with similar user requirements.

''(b) REALIGNMENT PLANS.—

''(1) IN GENERAL.—Not later than 60 days after selecting a system for the pilot program under subsection (a)(3), the Secretary shall develop a plan for realigning the system by breaking down the system into smaller increments using agile or iterative development methods. The realignment plan shall include a revised cost estimate that is lower than the cost estimate for the system that was current as of the date of the enactment of this Act [Dec. 12, 2017].

''(2) REALIGNMENT EXECUTION.—Each increment for a realigned system shall—

''(A) be designed to deliver a meaningfully useful capability within the first 180 days following realignment;

''(B) be designed to deliver subsequent meaningfully useful capabilities in time periods of less than 180 days;

''(C) incorporate multidisciplinary teams focused on software production that prioritize user needs and control of total cost of ownership;

''(D) be staffed with highly qualified technically trained staff and personnel with management and business process expertise in leadership positions to support requirements modification, acquisition strategy, and program decisionmaking;

''(E) ensure that the acquisition strategy for the realigned system is broad enough to allow for proposals of a service, system, modified business practice, configuration of personnel, or combination thereof for implementing the strategy;

''(F) include periodic engagement with the user community, as well as representation by the user community in program management and software production activity;

''(G) ensure that the acquisition strategy for the realigned system favors outcomes-based requirements definition and capability as a service, including the establishment of technical evaluation criteria as outcomes to be used to negotiate service-level agreements with vendors; and

''(H) consider options for termination of the relationship with any vendor unable or unwilling to offer terms that meet the requirements of this section.

''(c) REMOVAL OF SYSTEMS.—The Secretary may remove a system selected for the pilot program under subsection (a)(3) only after the Secretary submits to the Committees on Armed Services of the Senate and House of Representatives a written determination that indicates that the selected system has been unsuccessful in reducing cost or schedule growth, or is not meeting the overall needs of the pilot program.

''(d) EDUCATION AND TRAINING IN AGILE OR ITERATIVE DEVELOPMENT METHODS.—

''(1) TRAINING REQUIREMENT.—The Secretary shall ensure that any personnel from the relevant organizations in each of the military departments and Defense Agencies participating in the pilot program, including organizations responsible for engineering, budgeting, contracting, test and evaluation, requirements validation, and certification and accreditation, receive targeted training in agile or iterative development methods, including the interim course required by section 891 of this Act [10 U.S.C. 1746 note].

''(2) SUPPORT.—In carrying out the pilot program under subsection (a), the Secretary shall ensure that personnel participating in the program provide feedback to inform the development of education and training curricula as required by section 891.

''(e) SUNSET.—The pilot program required under subsection (a) shall terminate on September 30, 2023. Any system selected under subsection (a)(3) for the pilot program shall continue after that date through the execution of its realignment plan.

''(f) AGILE OR ITERATIVE DEVELOPMENT DEFINED.—In this section, the term 'agile or iterative development', with respect to software—

''(1) means acquisition pursuant to a method for delivering multiple, rapid, incremental capabilities to the user for operational use, evaluation, and feedback not exclusively linked to any single, proprietary method or process; and

''(2) involves—

''(A) the incremental development and fielding of capabilities, commonly called 'spirals', 'spins', or 'sprints', which can be measured in a few weeks or months; and

''(B) continuous participation and collaboration by users, testers, and requirements authorities.''

GLOBAL THEATER SECURITY COOPERATION MANAGEMENT INFORMATION SYSTEM

Pub. L. 115–91, div. A, title XII, § 1272, Dec. 12, 2017, 131 Stat. 1695, provided that:

''(a) UPDATE OF GUIDANCE.—

''(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act [Dec. 12, 2017], the Secretary of Defense shall—

''(A) update relevant security cooperation guidance issued by the Secretary for use of the Global Theater Security Cooperation Management Information System (in this section referred to as 'G-TSCMIS'), including guidance relating to the matters described in paragraph (3); and

''(B) submit to the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] a report that contains such guidance.

''(2) SUCCESSOR SYSTEM.—Not later than 180 days after the date of the adoption of any security cooperation information system that is a successor to G-TSCMIS, the Secretary of Defense shall—

''(A) update relevant security cooperation guidance issued by the Secretary for use of such system, including guidance relating to the matters described in paragraph (3); and

''(B) submit to the congressional defense committees a report that contains such guidance.

''(3) MATTERS DESCRIBED.—The matters described in this paragraph are the following:

''(A) Designation of an authoritative data repository for security cooperation information, with enforceable data standards and data controls.

''(B) Responsibilities for entry of data relating to programs and activities into the system.

''(C) Oversight and accountability measures to ensure the full scope of activities are entered into the system consistently and in a timely manner.

''(D) Such other matters as the Secretary considers appropriate.

''(b) REPORT.—

''(1) IN GENERAL.—Not later than 270 days after the adoption of any security cooperation information system that is the successor to G-TSCMIS, the Secretary of Defense shall submit to the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] a report setting forth a review of measures for evaluating the system in order to comply with guidance required by subsection (a).

''(2) ELEMENTS.—The review required by paragraph (1) shall include the following:

''(A) An evaluation of the impacts of inconsistent information on the system's functionality as a tool for planning, resource allocation, and adjustment.

''(B) An evaluation of the effectiveness of oversight and accountability measures.

''(C) An evaluation of feedback from the operational community to inform future requirements.

''(D) Such other matters as the Secretary considers appropriate.

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

GUIDANCE ON ACQUISITION OF BUSINESS SYSTEMS

Pub. L. 114–92, div. A, title VIII, § 883(e), Nov. 25, 2015, 129 Stat. 947, provided that: ''The Secretary of Defense shall issue guidance for major automated information systems acquisition programs to promote the use of best acquisition, contracting, requirement development, systems engineering, program management, and sustainment practices, including—

''(1) ensuring that an acquisition program baseline has been established within two years after program initiation;

''(2) ensuring that program requirements have not changed in a manner that increases acquisition costs or delays the schedule, without sufficient cause and only after maximum efforts to reengineer business processes prior to changing requirements;

''(3) policies to evaluate commercial off-the-shelf business systems for security, resilience, reliability, interoperability, and integration with existing interrelated systems where such system integration and interoperability are essential to Department of Defense operations;

''(4) policies to work with commercial off-the-shelf business system developers and owners in adapting systems for Department of Defense use;

''(5) policies to perform Department of Defense legacy system audits to determine which systems are related to or rely upon the system to be replaced or integrated with commercial off-the-shelf business systems;

''(6) policies to perform full backup of systems that will be changed or replaced by the installation of commercial off-the-shelf business systems prior to installation and deployment to ensure reconstitution of the system to a functioning state should it become necessary;

''(7) policies to engage the research and development activities and laboratories of the Department of Defense to improve acquisition outcomes; and

''(8) policies to refine and improve developmental and operational testing of business processes that are supported by the major automated information systems.''

DESIGNATION OF MILITARY DEPARTMENT ENTITY RESPONSIBLE FOR ACQUISITION OF CRITICAL CYBER CAPABILITIES

Pub. L. 114–92, div. A, title XVI, §1645, Nov. 25, 2015, 129 Stat. 1117, provided that:

''(a) DESIGNATION.—

''(1) IN GENERAL.—Not later than 90 days after the date of the enactment of this Act [Nov. 25, 2015], the Secretary of Defense shall designate an entity within a military department to be responsible for the acquisition of each critical cyber capability described in paragraph (2).

''(2) CRITICAL CYBER CAPABILITIES DESCRIBED.—The critical cyber capabilities described in this paragraph are the cyber capabilities that the Secretary considers critical to the mission of the Department of Defense, including the following:

''(A) The Unified Platform described in the Department of Defense document titled 'The Department of Defense Cyber Strategy' dated April 15, 2015.

''(B) A persistent cyber training environment.

''(C) A cyber situational awareness and battle management system.

''(b) REPORT.—

''(1) IN GENERAL.—Not later than 90 days after the date of the enactment of this Act, the Secretary shall submit to the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] a report containing the information described in paragraph (2).

''(2) CONTENTS.—The report under paragraph (1) shall include the following with respect to the critical cyber capabilities described in subsection (a)(2):

''(A) Identification of each critical cyber capability and the entity of a military department responsible for the acquisition of the capability.

''(B) Estimates of the funding requirements and acquisition timelines for each critical cyber capability.

''(C) An explanation of whether critical cyber capabilities could be acquired more quickly with changes to acquisition authorities.

''(D) Such recommendations as the Secretary may have for legislation or administrative action to improve the acquisition of, or to acquire more quickly, the critical cyber capabilities for which designations are made under subsection (a).''

MODULAR OPEN SYSTEMS APPROACHES IN ACQUISITION PROGRAMS

Pub. L. 113–291, div. A, title VIII, §801, Dec. 19, 2014, 128 Stat. 3425, provided that:

''(a) PLAN FOR MODULAR OPEN SYSTEMS APPROACH THROUGH DEVELOPMENT AND ADOPTION OF STANDARDS AND ARCHITECTURES.—Not later than January 1, 2016, the Under Secretary of Defense for Acquisition, Technology, and Logistics shall submit a report to the Committees on Armed Services of the Senate and the House of Representatives detailing a plan to develop standards and define architectures necessary to enable open systems approaches in the key mission areas of the Department of Defense with respect to which the Under Secretary determines that such standards and architectures would be feasible and cost effective.

''(b) CONSIDERATION OF MODULAR OPEN SYSTEMS APPROACHES.—

''(1) Review of acquisition guidance.—The Under Secretary of Defense for Acquisition, Technology, and Logistics shall review current acquisition guidance, and modify such guidance as necessary, to—

''(A) ensure that acquisition programs include open systems approaches in the product design and acquisition of information technology systems to the maximum extent practicable; and

''(B) for any information technology system not using an open systems approach, ensure that written justification is provided in the contract file for the system detailing why an open systems approach was not used.

''(2) ELEMENTS.—The review required in paragraph (1) shall—

''(A) consider whether the guidance includes appropriate exceptions for the acquisition of—

''(i) commercial items; and

''(ii) solutions addressing urgent operational needs;

''(B) determine the extent to which open systems approaches should be addressed in analysis of alternatives, acquisition strategies, system engineering plans, and life cycle sustainment plans; and

''(C) ensure that increments of acquisition programs consider the extent to which the increment will implement open systems approaches as a whole.

''(3) DEADLINE FOR REVIEW.—The review required in this subsection shall be completed no later than 180 days after the date of the enactment of this Act [Dec. 19, 2014].

''(c) TREATMENT OF ONGOING AND LEGACY PROGRAMS.—

''(1) REPORT REQUIREMENT.—Not later than one year after the date of the enactment of this Act, the Under Secretary of Defense for Acquisition, Technology, and Logistics shall submit to the Committees on Armed Services of the Senate and the House of Representatives a report covering the matters specified in paragraph (2).

''(2) MATTERS COVERED.—Subject to paragraph (3), the report required in this subsection shall—

''(A) identify all information technology systems that are in development, production, or deployed status as of the date of the enactment of this Act, that are or were major defense acquisition programs or major automated information systems, and that are not using an open systems approach;

''(B) identify gaps in standards and architectures necessary to enable open systems approaches in the key mission areas of the Department of Defense, as determined pursuant to the plan submitted under subsection (a); and

''(C) outline a process for potential conversion to an open systems approach for each information technology system identified under subparagraph (A).

''(3) LIMITATIONS.—The report required in this subsection shall not include information technology systems—

''(A) having a planned increment before fiscal year 2021 that will result in conversion to an open systems approach; and

''(B) that will be in operation for fewer than 15 years after the date of the enactment of this Act.

''(d) DEFINITIONS.—In this section:

''(1) INFORMATION TECHNOLOGY.—The term 'information technology' has the meaning given the term in section 11101(6) of title 40, United States Code.

''(2) OPEN SYSTEMS APPROACH.—The term 'open systems approach' means, with respect to an information technology system, an integrated business and technical strategy that—

''(A) employs a modular design and uses widely supported and consensus-based standards for key interfaces;

''(B) is subjected to successful validation and verification tests to ensure key interfaces comply with widely supported and consensus-based standards; and

''(C) uses a system architecture that allows components to be added, modified, replaced, removed, or supported by different vendors throughout the lifecycle of the system to afford opportunities for enhanced competition and innovation while yielding—

''(i) significant cost and schedule savings; and

''(ii) increased interoperability.''

OPERATIONAL METRICS FOR JOINT INFORMATION ENVIRONMENT AND SUPPORTING ACTIVITIES

Pub. L. 113–291, div. A, title VIII, § 854, Dec. 19, 2014, 128 Stat. 3459, provided that:

''(a) GUIDANCE.—Not later than 180 days after the date of the enactment of this Act [Dec. 19, 2014], the Secretary of Defense, acting through the Chief Information Officer of the Department of Defense, shall issue guidance for measuring the operational effectiveness and efficiency of the Joint Information Environment within the military departments, Defense Agencies, and combatant commands. The guidance shall include a definition of specific metrics for data collection, and a requirement for each military department, Defense Agency, and combatant command to regularly collect and assess data on such operational effectiveness and efficiency and report the results to such Chief Information Officer on a regular basis.

''(b) BASELINE ARCHITECTURE.—The Chief Information Officer of the Department of Defense shall identify a baseline architecture for the Joint Information Environment by identifying and reporting to the Secretary of Defense any information technology programs or other investments that support that architecture.

''(c) JOINT INFORMATION ENVIRONMENT DEFINED.—In this section, the term 'Joint Information Environment' means the initiative of the Department of Defense to modernize the information technology networks and systems within the Department.''

SUPERVISION OF THE ACQUISITION OF CLOUD COMPUTING CAPABILITIES

Pub. L. 113–66, div. A, title IX, § 938, Dec. 26, 2013, 127 Stat. 835, provided that:

''(a) SUPERVISION.—

''(1) IN GENERAL.—The Secretary of Defense shall, acting through the Under Secretary of Defense for Acquisition, Technology, and Logistics, the Under Secretary of Defense for Intelligence [now Under Secretary of Defense for Intelligence and Security], the Chief Information Officer of the Department of Defense, and the Chairman of the Joint Requirements Oversight Council, supervise the following:

''(A) Review, development, modification, and approval of requirements for cloud computing solutions for data analysis and storage by the Armed Forces and the Defense Agencies, including requirements for cross-domain, enterprise-wide discovery and correlation of data stored in cloud and non-cloud computing databases, relational and non-relational databases, and hybrid databases.

''(B) Review, development, modification, approval, and implementation of plans for the competitive acquisition of cloud computing systems or services to meet requirements described in subparagraph (A), including plans for the transition from current computing systems to systems or services acquired.

''(C) Development and implementation of plans to ensure that the cloud systems or services acquired pursuant to subparagraph (B) are interoperable and universally accessible and usable through attribute-based access controls.

''(D) Integration of plans under subparagraphs (B) and (C) with enterprise-wide plans of the Armed Forces and the Department of Defense for the Joint Information Environment and the Defense Intelligence Information Environment.

''(2) DIRECTION.—The Secretary shall provide direction to the Armed Forces and the Defense Agencies on the matters covered by paragraph (1) by not later than March 15, 2014.

''(b) INTEGRATION WITH INTELLIGENCE COMMUNITY EFFORTS.—The Secretary shall coordinate with the Director of National Intelligence to ensure that activities under this section are integrated with the Intelligence Community Information Technology Enterprise in order to achieve interoperability, information sharing, and other efficiencies.

''(c) LIMITATION.—The requirements of subparagraphs (B), (C), and (D) of subsection (a)(1) shall not apply to a contract for the acquisition of cloud computing capabilities in an amount less than $1,000,000.

''(d) RULE OF CONSTRUCTION.—Nothing in this section shall be construed to alter or affect the authorities or responsibilities of the Director of National Intelligence under section 102A of the National Security Act of 1947 (50 U.S.C. 3024).''

COMPETITION IN CONNECTION WITH DEPARTMENT OF DEFENSE TACTICAL DATA LINK SYSTEMS

Pub. L. 112–239, div. A, title IX, § 934, Jan. 2, 2013, 126 Stat. 1885, as amended by Pub. L. 113–66, div. A, title IX, § 931, Dec. 26, 2013, 127 Stat. 829, which provided that the upgrade, new deployment, or replacement of defense tactical data link systems should be open to competition, was repealed by Pub. L. 115–232, div. A, title VIII, § 812(b)(1), Aug. 13, 2018, 132 Stat. 1847.

DATA SERVERS AND CENTERS

Pub. L. 112–81, div. B, title XXVIII, § 2867, Dec. 31, 2011, 125 Stat. 1704, as amended by Pub. L. 112–239, div. B, title XXVIII, § 2853, Jan. 2, 2013, 126 Stat. 2161; Pub. L. 115–91, div. A, title X, § 1051(q)(3), Dec. 12, 2017, 131 Stat. 1565, provided that:

''(a) LIMITATIONS ON OBLIGATION OF FUNDS.—

''(1) LIMITATIONS.—

''(A) BEFORE PERFORMANCE PLAN.—During the period beginning on the date of the enactment of this Act [Dec. 31, 2011] and ending on May 1, 2012, a department, agency, or component of the Department of Defense may not obligate funds for a data server farm or data center unless approved by the Chief Information Officer of the Department of Defense or the Chief Information Officer of a component of the Department to whom the Chief Information Officer of the Department has specifically delegated such approval authority.

''(B) UNDER PERFORMANCE PLAN.—After May 1, 2012, a department, agency, or component of the Department may not obligate funds for a data center, or any information systems technology used therein, unless that obligation is in accordance with the performance plan required by subsection (b) and is approved as described in subparagraph (A).

''(2) REQUIREMENTS FOR APPROVALS.—

''(A) BEFORE PERFORMANCE PLAN.—An approval of the obligation of funds may not be granted under paragraph (1)(A) unless the official granting the approval determines, in writing, that existing resources of the agency, component, or element concerned cannot affordably or practically be used or modified to meet the requirements to be met through the obligation of funds.

''(B) UNDER PERFORMANCE PLAN.—An approval of the obligation of funds may not be granted under paragraph (1)(B) unless the official granting the approval determines that—

''(i) existing resources of the Department do not meet the operation requirements to be met through the obligation of funds; and

''(ii) the proposed obligation is in accordance with the performance standards and measures es-

tablished by the Chief Information Officer of the Department under subsection (b).

''(3) REPORTS.—Not later than 30 days after the end of each calendar quarter, each Chief Information Officer of a component of the Department who grants an approval under paragraph (1) during such calendar quarter shall submit to the Chief Information Officer of the Department a report on the approval or approvals so granted during such calendar quarter.

''(b) PERFORMANCE PLAN FOR REDUCTION OF RESOURCES REQUIRED FOR DATA SERVERS AND CENTERS.—

''(1) COMPONENT PLANS.—

''(A) IN GENERAL.—Not later than January 15, 2012, the Secretaries of the military departments and the heads of the Defense Agencies shall each submit to the Chief Information Officer of the Department a plan for the department or agency concerned to achieve the following:

''(i) A reduction in the square feet of floor space devoted to information systems technologies, attendant support technologies, and operations within data centers.

''(ii) A reduction in the use of all utilities necessary to power and cool information systems technologies and data centers.

''(iii) An increase in multi-organizational utilization of data centers, information systems technologies, and associated resources.

''(iv) A reduction in the investment for capital infrastructure or equipment required to support data centers as measured in cost per megawatt of data storage.

''(v) A reduction in the number of commercial and government developed applications running on data servers and within data centers.

''(vi) A reduction in the number of government and vendor provided full-time equivalent personnel, and in the cost of labor, associated with the operation of data servers and data centers.

''(B) SPECIFICATION OF REQUIRED ELEMENTS.—The Chief Information Officer of the Department shall specify the particular performance standards and measures and implementation elements to be included in the plans submitted under this paragraph, including specific goals and schedules for achieving the matters specified in subparagraph (A).

''(2) DEFENSE-WIDE PLAN.—

''(A) IN GENERAL.—Not later than April 1, 2012, the Chief Information Officer of the Department shall submit to the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] a performance plan for a reduction in the resources required for data centers and information systems technologies Department-wide. The plan shall be based upon and incorporate appropriate elements of the plans submitted under paragraph (1).

''(B) ELEMENTS.—The performance plan required under this paragraph shall include the following:

''(i) A Department-wide performance plan for achieving the matters specified in paragraph (1)(A), including performance standards and measures for data centers and information systems technologies, goals and schedules for achieving such matters, and an estimate of cost savings anticipated through implementation of the plan.

''(ii) A Department-wide strategy for each of the following:

''(I) Desktop, laptop, and mobile device virtualization.

''(II) Transitioning to cloud computing.

''(III) Migration of Defense data and government-provided services from Department-owned and operated data centers to cloud computing services generally available within the private sector that provide a better capability at a lower cost with the same or greater degree of security.

''(IV) Utilization of private sector-managed security services for data centers and cloud computing services.

''(V) A finite set of metrics to accurately and transparently report on data center infrastructure (space, power and cooling): age, cost, capacity, usage, energy efficiency and utilization, accompanied with the aggregate data for each data center site in use by the Department in excess of 100 kilowatts of information technology power demand.

''(VI) Transitioning to just-in-time delivery of Department-owned data center infrastructure (space, power and cooling) through use of modular data center technology and integrated data center infrastructure management software.

''(3) RESPONSIBILITY.—The Chief Information Officer of the Department shall discharge the responsibility for establishing performance standards and measures for data centers and information systems technologies for purposes of this subsection. Such responsibility may not be delegated.

''(c) EXCEPTIONS.—

''(1) INTELLIGENCE COMPONENTS.—The Chief Information Officer of the Department and the Chief Information Officer of the Intelligence Community may jointly exempt from the applicability of this section such intelligence components of the Department of Defense (and the programs and activities thereof) that are funded through the National Intelligence Program (NIP) as the Chief Information Officers consider appropriate.

''(2) RESEARCH, DEVELOPMENT, TEST, AND EVALUATION PROGRAMS.—The Chief Information Officer of the Department may exempt from the applicability of this section research, development, test, and evaluation programs that use authorization of appropriations for the High Performance Computing Modernization Program (Program Element 0603461A) if the Chief Information Officer determines that the exemption is in the best interest of national security.''

DEMONSTRATION AND PILOT PROJECTS ON CYBERSECURITY

Pub. L. 111–383, div. A, title II, §215, Jan. 7, 2011, 124 Stat. 4165, provided that:

''(a) DEMONSTRATION PROJECTS ON PROCESSES FOR APPLICATION OF COMMERCIAL TECHNOLOGIES TO CYBERSECURITY REQUIREMENTS.—

''(1) PROJECTS REQUIRED.—The Secretary of Defense and the Secretaries of the military departments shall jointly carry out demonstration projects to assess the feasibility and advisability of using various business models and processes to rapidly and effectively identify innovative commercial technologies and apply such technologies to Department of Defense and other cybersecurity requirements.

''(2) SCOPE OF PROJECTS.—Any demonstration project under paragraph (1) shall be carried out in such a manner as to contribute to the cyber policy review of the President and the Comprehensive National Cybersecurity Initiative.

''(b) PILOT PROGRAMS ON CYBERSECURITY REQUIRED.—The Secretary of Defense shall support or conduct pilot programs on cybersecurity with respect to the following areas:

''(1) Threat sensing and warning for information networks worldwide.

''(2) Managed security services for cybersecurity within the defense industrial base, military departments, and combatant commands.

''(3) Use of private processes and infrastructure to address threats, problems, vulnerabilities, or opportunities in cybersecurity.

''(4) Processes for securing the global supply chain.

''(5) Processes for threat sensing and security of cloud computing infrastructure.

''(c) REPORTS.—

''(1) REPORTS REQUIRED.—Not later than 240 days after the date of the enactment of this Act [Jan. 7, 2011], and annually thereafter at or about the time of the submittal to Congress of the budget of the President for a fiscal year (as submitted pursuant to sec-

tion 1105(a) of title 31, United States Code), the Secretary of Defense shall, in coordination with the Secretary of Homeland Security, submit to Congress a report on any demonstration projects carried out under subsection (a), and on the pilot projects carried out under subsection (b), during the preceding year.

''(2) ELEMENTS.—Each report under this subsection shall include the following:

''(A) A description and assessment of any activities under the demonstration projects and pilot projects referred to in paragraph (1) during the preceding year.

''(B) For the pilot projects supported or conducted under subsection (b)(2)—

''(i) a quantitative and qualitative assessment of the extent to which managed security services covered by the pilot project could provide effective and affordable cybersecurity capabilities for components of the Department of Defense and for entities in the defense industrial base, and an assessment whether such services could be expanded rapidly to a large scale without exceeding the ability of the Federal Government to manage such expansion; and

''(ii) an assessment of whether managed security services are compatible with the cybersecurity strategy of the Department of Defense with respect to conducting an active, in-depth defense under the direction of United States Cyber Command.

''(C) For the pilot projects supported or conducted under subsection (b)(3)—

''(i) a description of any performance metrics established for purposes of the pilot project, and a description of any processes developed for purposes of accountability and governance under any partnership under the pilot project; and

''(ii) an assessment of the role a partnership such as a partnership under the pilot project would play in the acquisition of cyberspace capabilities by the Department of Defense, including a role with respect to the development and approval of requirements, approval and oversight of acquiring capabilities, test and evaluation of new capabilities, and budgeting for new capabilities.

''(D) For the pilot projects supported or conducted under subsection (b)(4)—

''(i) a framework and taxonomy for evaluating practices that secure the global supply chain, as well as practices for securely operating in an uncertain or compromised supply chain;

''(ii) an assessment of the viability of applying commercial practices for securing the global supply chain; and

''(iii) an assessment of the viability of applying commercial practices for securely operating in an uncertain or compromised supply chain.

''(E) For the pilot projects supported or conducted under subsection (b)(5)—

''(i) an assessment of the capabilities of Federal Government providers to offer secure cloud computing environments; and

''(ii) an assessment of the capabilities of commercial providers to offer secure cloud computing environments to the Federal Government.

''(3) FORM.—Each report under this subsection shall be submitted in unclassified form, but may include a classified annex.''

IMPLEMENTATION OF NEW ACQUISITION PROCESS FOR INFORMATION TECHNOLOGY SYSTEMS

Pub. L. 111–84, div. A, title VIII, § 804, Oct. 28, 2009, 123 Stat. 2402, which provided for development and implementation of a new acquisition process for information technology systems, was repealed by Pub. L. 115–232, div. A, title VIII, § 812(b)(2), Aug. 13, 2018, 132 Stat. 1848.

CLEARINGHOUSE FOR RAPID IDENTIFICATION AND DISSEMINATION OF COMMERCIAL INFORMATION TECHNOLOGIES

Pub. L. 110–181, div. A, title VIII, § 881, Jan. 28, 2008, 122 Stat. 262, provided that:

''(a) REQUIREMENT TO ESTABLISH CLEARINGHOUSE.—Not later than 180 days after the date of the enactment of this Act [Jan. 28, 2008], the Secretary of Defense, acting through the Assistant Secretary of Defense for Networks and Information Integration, shall establish a clearinghouse for identifying, assessing, and disseminating knowledge about readily available information technologies (with an emphasis on commercial off-the-shelf information technologies) that could support the warfighting mission of the Department of Defense.

''(b) RESPONSIBILITIES.—The clearinghouse established pursuant to subsection (a) shall be responsible for the following:

''(1) Developing a process to rapidly assess and set priorities and needs for significant information technology needs of the Department of Defense that could be met by commercial technologies, including a process for—

''(A) aligning priorities and needs with the requirements of the commanders of the combatant command; and

''(B) proposing recommendations to the commanders of the combatant command of feasible technical solutions for further evaluation.

''(2) Identifying and assessing emerging commercial technologies (including commercial off-the-shelf technologies) that could support the warfighting mission of the Department of Defense, including the priorities and needs identified pursuant to paragraph (1).

''(3) Disseminating information about commercial technologies identified pursuant to paragraph (2) to commanders of combatant commands and other potential users of such technologies.

''(4) Identifying gaps in commercial technologies and working to stimulate investment in research and development in the public and private sectors to address those gaps.

''(5) Enhancing internal data and communications systems of the Department of Defense for sharing and retaining information regarding commercial technology priorities and needs, technologies available to meet such priorities and needs, and ongoing research and development directed toward gaps in such technologies.

''(6) Developing mechanisms, including web-based mechanisms, to facilitate communications with industry regarding the priorities and needs of the Department of Defense identified pursuant to paragraph (1) and commercial technologies available to address such priorities and needs.

''(7) Assisting in the development of guides to help small information technology companies with promising technologies to understand and navigate the funding and acquisition processes of the Department of Defense.

''(8) Developing methods to measure how well processes developed by the clearinghouse are being utilized and to collect data on an ongoing basis to assess the benefits of commercial technologies that are procured on the recommendation of the clearinghouse.

''(c) PERSONNEL.—The Secretary of Defense, acting through the Assistant Secretary of Defense for Networks and Information Integration, shall provide for the hiring and support of employees (including detailees from other components of the Department of Defense and from other Federal departments or agencies) to assist in identifying, assessing, and disseminating information regarding commercial technologies under this section.

''(d) REPORT TO CONGRESS.—Not later than one year after the date of the enactment of this Act [Jan. 28, 2008], the Secretary of Defense shall submit to the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] a report on the implementation of this section.''

§ 2224. Defense Information Assurance Program

(a) DEFENSE INFORMATION ASSURANCE PROGRAM.—The Secretary of Defense shall carry out