''(A) develop a capability to communicate clearly and authoritatively about threats by foreign adversaries;

''(B) conduct independent red-team security analysis of systems, subsystems, devices, and components of the Department of Defense including no-knowledge testing and testing with limited or full knowledge of expected functionalities;

''(C) verify the integrity of personnel who are tasked with design fabrication, integration, configuration, storage, test, and documentation of non-commercial 5G technology to be used by the Department;

''(D) verify the efficacy of the physical security measures used at Department locations where system design, fabrication, integration, configuration, storage, test, and documentation of 5G technology occurs;

''(E) direct the Chief Information Officer to assess, using existing government evaluation models and schema where applicable, 5G core service providers whose services will be used by the Department through the Department's provisional authorization process; and

''(F) direct the Defense Information Systems Agency and the United States Cyber Command to develop a capability for continuous, independent monitoring of non-commercial, government-transiting packet streams for 5G data on frequencies assigned to the Department to validate the availability, confidentiality, and integrity of the Department's communications systems.

''(3) IMPLEMENTATION PLAN.—Not later than 90 days after the date of the enactment of this Act [Jan. 1, 2021], the Secretary of Defense shall submit to Congress a plan for the implementation of the program under paragraph (1).

''(4) REPORT.—Not later than 270 days after submitting the plan under paragraph (3), the Secretary of Defense shall submit to Congress a report that includes—

''(A) a comprehensive assessment of the findings and conclusions of the program under paragraph (1);

''(B) recommendations on how to mitigate vulnerabilities in the telecommunications infrastructure of the Department of Defense; and

''(C) an explanation of how the Department plans to implement such recommendations.

''(h) RULE OF CONSTRUCTION.—

''(1) IN GENERAL.—Nothing in this section shall be construed as providing the Chief Information Officer immediate responsibility for the activities of the Department of Defense in fifth-generation wireless networking experimentation and science and technology development.

''(2) PURVIEW OF EXPERIMENTATION AND SCIENCE AND TECHNOLOGY DEVELOPMENT.—The activities described in paragraph (1) shall remain within the purview of the Under Secretary of Defense for Research and Engineering, but shall inform and be informed by the activities of the cross-functional team established pursuant to subsection (c).''

DEMONSTRATION PROJECT ON USE OF CERTAIN TECHNOLOGIES FOR FIFTH-GENERATION WIRELESS NETWORKING SERVICES

Pub. L. 116–283, div. A, title II, § 225, Jan. 1, 2021, 134 Stat. 3475, provided that:

''(a) DEMONSTRATION PROJECT.—The Secretary of Defense shall carry out a demonstration project to evaluate the maturity, performance, and cost of covered technologies to provide additional options for providers of fifth-generation wireless network services.

''(b) LOCATION.—The Secretary of Defense shall carry out the demonstration project under subsection (a) in at least one location where the Secretary plans to deploy a fifth-generation wireless network.

''(c) COORDINATION.—The Secretary shall carry out the demonstration project under subsection (a) in coordination with at least one major wireless network service provider based in the United States.

''(d) COVERED TECHNOLOGIES DEFINED.—In this section, the term 'covered technologies' means—

''(1) a disaggregated or virtualized radio access network and core in which components can be provided by different vendors and interoperate through open protocols and interfaces, including those protocols and interfaces utilizing the Open Radio Access Network (commonly known as 'Open RAN' or 'oRAN') approach; and

''(2) one or more massive multiple-input, multiple-output radio arrays, provided by one or more companies based in the United States, that have the potential to compete favorably with radios produced by foreign companies in terms of cost, performance, and efficiency.''

PILOT PROGRAM ON THE USE OF CONSUMPTION-BASED SOLUTIONS TO ADDRESS SOFTWARE-INTENSIVE WARFIGHTING CAPABILITY

Pub. L. 116–283, div. A, title VIII, § 834, Jan. 1, 2021, 134 Stat. 3754, provided that:

''(a) IN GENERAL.—Subject to the availability of appropriations, the Secretary of Defense is authorized to establish a pilot program to explore the use of consumption-based solutions to address software-intensive warfighting capability.

''(b) SELECTION OF INITIATIVES.—Each Secretary of a military department and each commander of a combatant command with acquisition authority shall propose for selection by the Secretary of Defense for the pilot program at least one and not more than three initiatives that are well-suited to explore consumption-based solutions, to include addressing software-intensive warfighting capability. The initiatives may be new or existing programs of record, and may include applications that—

''(1) rapidly analyze sensor data;

''(2) secure warfighter networks, including multi-level security;

''(3) swiftly transport information across various networks and network modalities;

''(4) enable joint all-domain operational concepts, including in a contested environment; or

''(5) advance military capabilities and effectiveness.

''(c) REQUIREMENTS.—A contract or other agreement for consumption-based solutions entered into under the pilot program shall require—

''(1) the effectiveness of the solution to be measurable at regular intervals customary for the type of solution provided under contract or other agreement; and

''(2) that the awardee notify the Secretary of Defense when consumption under the contract or other agreement reaches 75 percent and 90 percent of the funded amount, respectively, of the contract or other agreement.

''(d) EXEMPTION.—A modification to a contract or other agreement entered into under this section to add new features or capabilities in an amount less than or equal to 25 percent of the total value of such contract or other agreement shall be exempt from the requirements of full and open competition (as defined in section 2302 of title 10, United States Code [see 10 U.S.C. 3011]).

''(e) DURATION.—The duration of a contract or other agreement entered into under this section may not exceed three years.

''(f) MONITORING AND EVALUATION OF PILOT PROGRAM.—The Director of Cost Assessment and Program Evaluation shall continuously monitor and evaluate the pilot program, including by collecting data on cost, schedule, and performance from the program office, the user community, and the awardees involved in the program.

''(g) REPORTS.—

''(1) INITIAL REPORT.—Not later than May 15, 2021, 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 initiatives se-

lected for the pilot program, roles, and responsibilities for implementing the program, and the monitoring and evaluation approach that will be used for the program.

''(2) PROGRESS REPORT.—Not later than October 15, 2021, the Secretary of Defense shall submit to the congressional defense committees a report on the progress of the initiatives selected for the pilot program.

''(3) FINAL REPORT.—Not later than 3 years after the date of the enactment of this Act [Jan. 1, 2021], the Secretary of Defense shall submit to the congressional defense committees a report on the cost, schedule, and performance outcomes of the initiatives carried out under the pilot program. The report shall also include lessons learned about the use of consumption-based solutions for software-intensive capabilities and any recommendations for statutory or regulatory changes to facilitate the use of such solutions.

''(h) CONSUMPTION-BASED SOLUTION DEFINED.—In this section, the term 'consumption-based solution' means any combination of software, hardware or equipment, and labor or services that provides a seamless capability that is metered and billed based on actual usage and predetermined pricing per resource unit, and includes the ability to rapidly scale capacity up or down.''

BALANCING SECURITY AND INNOVATION IN SOFTWARE DEVELOPMENT AND ACQUISITION

Pub. L. 116–283, div. A, title VIII, §835, Jan. 1, 2021, 134 Stat. 3755, provided that:

''(a) REQUIREMENTS FOR SOLICITATIONS OF COMMERCIAL AND DEVELOPMENTAL SOLUTIONS.—The Under Secretary of Defense for Acquisition and Sustainment, in coordination with the Chief Information Officer of the Department of Defense, shall develop requirements for appropriate software security criteria to be included in solicitations for commercial and developmental solutions and the evaluation of bids submitted in response to such solicitations, including a delineation of what processes were or will be used for a secure software development life cycle. Such requirements shall include—

''(1) establishment and enforcement of secure coding practices;

''(2) management of supply chain risks and third-party software sources and component risks;

''(3) security of the software development environment;

''(4) secure deployment, configuration, and installation processes; and

''(5) an associated vulnerability management plan and identification of tools that will be applied to achieve an appropriate level of security.

''(b) SECURITY REVIEW OF CODE.—The Under Secretary of Defense for Acquisition and Sustainment, in coordination with the Chief Information Officer of the Department of Defense, shall develop—

''(1) procedures for the security review of code; and

''(2) other procedures necessary to fully implement the pilot program required under section 875 of the National Defense Authorization Act for Fiscal Year 2018 (Public Law 115–91; 10 U.S.C. 2223 note).

''(c) COORDINATION WITH CYBERSECURITY ACQUISITION POLICY EFFORTS.—The Under Secretary of Defense for Acquisition and Sustainment shall develop the requirements and procedures described under subsections (a) and (b) in coordination with the efforts of the Department of Defense to develop new cybersecurity and program protection policies and guidance that are focused on cybersecurity in the context of acquisition and program management and on safeguarding information.''

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