118TH CONGRESS
2D SESSION

S. _____

To address security vulnerabilities with respect to unmanned aircraft systems used by civilian Federal agencies, and for other purposes.

IN THE SENATE OF THE UNITED STATES

Mr. WARNER (for himself and Mr. THUNE) introduced the following bill; which was read twice and referred to the Committee on _____

A BILL

To address security vulnerabilities with respect to unmanned aircraft systems used by civilian Federal agencies, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Drone Evaluation to Eliminate Cyber Threats Act'' or the ''DETECT Act''.

SEC. 2. DEFINITIONS.

In this Act:

(1) AGENCY.—The term ''agency'' has the meaning given the term in section 3502 of title 44, United States Code.

(2) CRITICAL COMPONENT.—The term ''critical component'' includes a flight controller, a radio, a data transmission device, a camera, a gimbal, a ground control system, operating software, network connectivity, and data storage.

(3) DIRECTOR.—The term ''Director'' means the Director of the Office of Management and Budget.

(4) INFORMATION SYSTEM.—The term ''information system'' has the meaning given the term in section 3502 of title 44, United States Code.

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

(6) SECRETARY.—The term ''Secretary'' means the Secretary of Homeland Security.

(7) SECURITY VULNERABILITY.—The term ''security vulnerability'' has the meaning given the term in section 2200 of the Homeland Security Act of 2002 (6 U.S.C. 650).

(8) UNDER SECRETARY.—The term ''Under Secretary'' means the Under Secretary of Commerce for Standards and Technology.

(9) UNMANNED AIRCRAFT SYSTEM.—The term ''unmanned aircraft system'' has the meaning given the term in section 331 of the FAA Modernization and Reform Act of 2012 (49 U.S.C. 44802 note).

SEC. 3. SECURITY GUIDELINES FOR FEDERAL AGENCIES ON USE AND MANAGEMENT OF UNMANNED AIRCRAFT SYSTEMS.

(a) NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY DEVELOPMENT OF STANDARDS AND GUIDELINES FOR FEDERAL USE OF UNMANNED AIRCRAFT SYSTEMS BY AGENCIES.—

(1) IN GENERAL.—Not later than 90 days after the date of the enactment of this Act, the Under Secretary shall commence the development of guidelines for the Federal Government on the appropriate use and management by agencies of unmanned aircraft systems owned or controlled by an agency and regularly connected to or exchanging data with information systems owned or controlled by an agency, including minimum information security requirements for managing cybersecurity risks associated with such devices.

(2) PUBLICATION.—Not later than 1 year after the date of the enactment of this Act, the Under Secretary shall publish the guidelines developed pursuant to paragraph (1) in a manner that is consistent with section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3).

(3) CONSISTENCY WITH ONGOING EFFORTS.—The Under Secretary shall ensure that the standards and guidelines developed under paragraph (1) are consistent with the efforts of the National Institute of Standards and Technology in effect on the date of the enactment of this Act—

(A) regarding—

(i) examples of possible security vulnerabilities of unmanned aircraft systems; and

(ii) considerations for managing the security vulnerabilities of unmanned aircraft systems; and

(B) with respect to the following considerations for unmanned aircraft systems:

(i) Secure Development.

(ii) Identity management.

(iii) Patch management.

(iv) Configuration management.

(v) Supply chain security.

(vi) Corporate cyber hygiene.

(vii) Software and hardware transparency.

(4) CONSIDERING RELEVANT GUIDELINES.—In developing the guidelines under paragraph (1), the Under Secretary shall consider relevant standards, guidelines, and best practices developed by the private sector, agencies, and public-private partnerships, including the following:

(A) National Institute of Standards and Technology Special Publication 800–213 (relating to IoT device cybersecurity guidance for the Federal Government).

(B) National Institute of Standards and Technology Special Publication 800–37 (relating to risk management framework for information systems and organizations).

(C) The Green UAS Frameworks of the Association for Uncrewed Vehicle Systems International (AUVSI), as amended and extended.

(D) The Cross-Sector Cybersecurity Performance Goals of The Cybersecurity and Infrastructure Security Agency.

(5) CONSULTATION.—In developing the guidelines required by paragraph (1), the Under Secretary shall consult with the Administrator of the Federal Aviation Administration, the Attorney General, and the heads of such other departments and agencies of the Federal Government as the Under Secretary considers appropriate.

(b) REVIEW OF FEDERAL AGENCY INFORMATION SECURITY POLICIES AND PRINCIPLES.—

(1) REQUIREMENT.—

(A) IN GENERAL.—Not later than 1 year after the date on which the Under Secretary completes the development of the guidelines required under subsection (a), the Director shall require not less than 1 agency, on a pilot basis, to implement policies and principles based on the guidelines with respect to unmanned aircraft systems owned or controlled by the agency.

(B) EXCEPTION.—A pilot implementation under subparagraph (A) shall not apply to any unmanned aircraft system comprised of any national security system.

(2) POLICIES AND PRINCIPLES.—Not later than 1 year after the conclusion of the pilot implementa-

tion under paragraph (1)(A), the Director shall issue policies and principles necessary to ensure that the policies and principles of each agency relating to the cybersecurity of unmanned aircraft systems are consistent with the guidelines developed under subsection (a).

(3) NATIONAL SECURITY SYSTEMS.—Any policy or principle issued by the Director under paragraph (2) shall not apply to national security systems.

(c) QUINQUENNIAL REVIEW AND REVISION.—

(1) REVIEW AND REVISION OF NIST GUIDELINES.—Not later than 5 years after the date on which the Under Secretary publishes the guidelines under subsection (a), and not less frequently than once every 5 years thereafter, the Under Secretary, shall—

(A) review such guidelines; and

(B) revise such guidelines as the Under Secretary considers appropriate.

(2) UPDATED OMB POLICIES AND PRINCIPLES FOR FEDERAL AGENCIES.—Not later than 180 days after the Under Secretary makes a revision pursuant to paragraph (1), the Director, in consultation with the Director of the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Se-

curity, shall update any policy or principle issued under subsection (b)(1) as necessary to ensure those policies and principles are consistent with the review and any revision under paragraph (1) under this subsection and paragraphs (2) and (3) of subsection (b).

(d) REVISION OF FEDERAL ACQUISITION REGULATION.—The Federal Acquisition Regulation shall be revised as necessary to implement any standards and guidelines promulgated in this section.

SEC. 4. GUIDELINES ON THE DISCLOSURE PROCESS FOR SECURITY VULNERABILITIES RELATING TO UNMANNED AIRCRAFT SYSTEMS.

(a) IN GENERAL.—

(1) GUIDANCE.—The Director shall issue guidance to agencies that includes—

(A) requirements for the reporting, coordinating, and receiving of information about—

(i) a security vulnerability relating to an unmanned aircraft system owned or controlled by an agency; and

(ii) the resolution of a security vulnerability described in clause (i); and

(B) requirements relating to the scope of vulnerabilities required to be reported under

subparagraph (A), such as the minimum severity of a vulnerability required to be reported or whether vulnerabilities that are publicly disclosed are required to be reported.

(2) CONTRACTOR COMPLIANCE WITH COORDINATED DISCLOSURE OF SECURITY VULNERABILITIES RELATING TO AGENCY UNMANNED AIRCRAFT SYSTEMS.—Subject to the guidance issued under paragraph (1), a contractor or awardee of an agency shall report to the agency and the Director of the Cybersecurity and Infrastructure Security Agency if—

(A) a critical component of any unmanned aircraft system operated, managed, or maintained by the contractor or awardee contains a security vulnerability, including a supply chain compromise or an identified software or hardware vulnerability, for which there is reliable evidence of attempted or successful exploitation by an actor without the authorization of the owner of the unmanned aircraft system; or

(B) the contractor or awardee has a reasonable basis to suspect or conclude that a critical component of any unmanned aircraft system operated, managed, or maintained on be-

half of an agency by the contractor or awardee contains a security vulnerability, including a supply chain compromise or an identified software or hardware vulnerability, that has been reported to the contractor or awardee by a third party, including through a vulnerability disclosure program.

(b) REGULATIONS; MODIFICATIONS.—

(1) IN GENERAL.—Not later than 1 year after the date of enactment of this Act—

(A) the Federal Acquisition Regulatory Council shall promulgate regulations, as appropriate, relating to the responsibilities of contractors and recipients of other transaction agreements and cooperative agreements to comply with subsection (a)(2); and

(B) the Office of Federal Financial Management shall promulgate regulations under title 2, Code of Federal Regulations, as appropriate, relating to the responsibilities of grantees to comply with subsection (a)(2).

(2) IMPLEMENTATION.—Not later than 1 year after the date on which the Federal Acquisition Regulatory Council and the Office of Federal Financial Management promulgate regulations under para-

graph (1), the head of each agency shall implement policies and procedures, as appropriate, necessary to implement those regulations.

(c) RESPONSIBILITIES OF CISA.—The Director of the Cybersecurity and Infrastructure Security Agency shall—

(1) provide support to agencies with respect to the implementation of the requirements of this section;

(2) develop tools, processes, and other mechanisms determined appropriate to offer agencies capabilities to implement the requirements of this section; and

(3) upon request by an agency, assist the agency in the disclosure to vendors of newly identified security vulnerabilities in vendor products and services.

SEC. 5. CONTRACTOR COMPLIANCE WITH COORDINATED DISCLOSURE OF SECURITY VULNERABILITIES RELATING TO AGENCY UNMANNED AIRCRAFT SYSTEMS.

(a) PROHIBITION ON PROCUREMENT AND USE.—

(1) IN GENERAL.—Subject to paragraph (2), the head of an agency may not procure or obtain, renew a contract to procure or obtain, or use an un-

manned aircraft system if the Chief Information Officer of the agency determines, in conducting the review required under section 11319(b)(1)(C) of title 40, United States Code, of the contract for the unmanned aircraft system, that the use of the unmanned aircraft system prevents compliance with the standards and guidelines developed under section 3(a)(1) of this Act or the guidelines issued under section 4(a)(1) of this Act with respect to the unmanned aircraft system.

(2) EXEMPTION FOR COMMERCIAL DATA BUYS.—Paragraph (1) shall not apply when the head of an acquires data—

(A) solely from a commercial or nonprofit entity, the contract or agreement for which does not specify the type of unmanned aircraft system or the specifications for the unmanned aircraft system;

(B) that will never connect to any network of the Federal Government; and

(C) over which the head of the agency will not have operational direction or control.

(3) SIMPLIFIED ACQUISITION THRESHOLD.—Notwithstanding section 1905 of title 41, United States Code, the requirements under paragraph (1)

shall apply to a contract or subcontract in amounts not greater than the simplified acquisition threshold.

(b) WAIVER.—

(1) AUTHORITY.—The head of an agency may waive the prohibition under subsection (a)(1) with respect to an unmanned aircraft system if the Chief Information Officer of that agency determines that—

(A) the waiver is necessary in the interest of national security;

(B) procuring, obtaining, or using the unmanned aircraft system is necessary for research, testing, evaluation, or training purposes; or

(C) the unmanned aircraft system is used—

(i) in a manner that does not implicate agency operational or cybersecurity concerns; or

(ii) in other circumstances in which the head of the agency determines the risks are minimal or acceptable.

(2) AGENCY PROCESS.—The Director shall establish a standardized process for the Chief Information Officer of each agency to follow in deter-

mining whether the waiver under paragraph (1) may be granted.

(c) REPORTS TO CONGRESS.—

(1) REPORT.—Not later than 2 years after the date of enactment of this Act, and every 2 years thereafter until the date that is 6 years after the date of enactment of this Act, the Comptroller General of the United States, in consultation with the heads of other Federal agencies as appropriate, shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate, the Committee on Oversight and Accountability of the House of Representatives, and the Committee on Homeland Security of the House of Representatives a report—

(A) on the effectiveness of the process established under subsection (b)(2);

(B) that contains recommended best practices for the procurement of unmanned aircraft systems; and

(C) that lists—

(i) the number and type of each unmanned aircraft system for which a waiver under subsection (b)(1) was granted during the 2-year period prior to the submission of the report; and

(ii) the legal authority under which each such waiver was granted, such as whether the waiver was granted pursuant to subparagraph (A), (B), or (C) of subsection (b).

(2) CLASSIFICATION OF REPORT.—Each report submitted under this subsection shall be submitted in unclassified form, but may include—

(A) a classified annex that contains the information described in paragraph (1)(C); and

(B) a committee-use only annex that contains information described in paragraph (1)(C) that is law enforcement sensitive.

(d) EFFECTIVE DATE.—The prohibition under subsection (a)(1) shall take effect on the date that is 2 years after the date of enactment of this Act.

SEC. 6. GOVERNMENT ACCOUNTABILITY OFFICE REPORT ON CYBERSECURITY CONSIDERATIONS OF UNMANNED AIRCRAFT SYSTEMS.

(a) BRIEFING.—Not later than 1 year after the date of enactment of this Act, the Comptroller General of the United States shall provide a briefing to the Committee on Homeland Security and Governmental Affairs of the Senate, the Committee on Oversight and Accountability of the House of Representatives, and the Committee on

Homeland Security of the House of Representatives on broader unmanned aircraft system cybersecurity efforts.

(b) REPORT.—Not later than 2 years after the date of enactment of this Act, the Comptroller General of the United States shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate, the Committee on Oversight and Accountability of the House of Representatives, and the Committee on Homeland Security of the House of Representatives a report on broader unmanned aircraft system cybersecurity efforts addressed in the briefing required under subsection (a).