

118TH CONGRESS  
2D SESSION

# S. 3758

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

FEBRUARY 7, 2024

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

---

## A BILL

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

1 *Be it enacted by the Senate and House of Representa-*  
2 *tives of the United States of America in Congress assembled,*

3 **SECTION 1. SHORT TITLE.**

4 This Act may be cited as the “Drone Evaluation To  
5 Eliminate Cyber Threats Act” or the “DETECT Act”.

6 **SEC. 2. DEFINITIONS.**

7 In this Act:

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

4           (2) CRITICAL COMPONENT.—The term “critical  
5 component” includes a flight controller, a radio, a  
6 data transmission device, a camera, a gimbal, a  
7 ground control system, operating software, network  
8 connectivity, and data storage.

9           (3) DIRECTOR.—The term “Director” means  
10 the Director of the Office of Management and Budget.  
11 et.

12           (4) INFORMATION SYSTEM.—The term “infor-  
13 mation system” has the meaning given the term in  
14 section 3502 of title 44, United States Code.

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

19           (6) SECRETARY.—The term “Secretary” means  
20 the Secretary of Homeland Security.

21           (7) SECURITY VULNERABILITY.—The term “se-  
22 curity vulnerability” has the meaning given the term  
23 in section 2200 of the Homeland Security Act of  
24 2002 (6 U.S.C. 650).

1           (8) UNDER SECRETARY.—The term “Under  
2       Secretary” means the Under Secretary of Commerce  
3       for Standards and Technology.

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

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

11       (a) NATIONAL INSTITUTE OF STANDARDS AND  
12       TECHNOLOGY DEVELOPMENT OF STANDARDS AND  
13       GUIDELINES FOR FEDERAL USE OF UNMANNED AIR-  
14       CRAFT SYSTEMS BY AGENCIES.—

15           (1) IN GENERAL.—Not later than 90 days after  
16       the date of the enactment of this Act, the Under  
17       Secretary shall commence the development of guide-  
18       lines for the Federal Government on the appropriate  
19       use and management by agencies of unmanned air-  
20       craft systems owned or controlled by an agency and  
21       regularly connected to or exchanging data with in-  
22       formation systems owned or controlled by an agency,  
23       including minimum information security require-  
24       ments for managing cybersecurity risks associated  
25       with such devices.

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

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

13                 (A) regarding—

14                         (i) examples of possible security  
15                         vulnerabilities of unmanned aircraft sys-  
16                         tems; and

17                         (ii) considerations for managing the  
18                         security vulnerabilities of unmanned air-  
19                         craft systems; and

20                 (B) with respect to the following consider-  
21          ations for unmanned aircraft systems:

22                         (i) Secure Development.

23                         (ii) Identity management.

24                         (iii) Patch management.

25                         (iv) Configuration management.

- 1 (v) Supply chain security.
- 2 (vi) Corporate cyber hygiene.
- 3 (vii) Software and hardware trans-
- 4 parency.

5 (4) CONSIDERING RELEVANT GUIDELINES.—In  
6 developing the guidelines under paragraph (1), the  
7 Under Secretary shall consider relevant standards,  
8 guidelines, and best practices developed by the pri-  
9 vate sector, agencies, and public-private partner-  
10 ships, including the following:

11 (A) National Institute of Standards and  
12 Technology Special Publication 800–213 (relat-  
13 ing to IoT device cybersecurity guidance for the  
14 Federal Government).

15 (B) National Institute of Standards and  
16 Technology Special Publication 800–37 (relat-  
17 ing to risk management framework for informa-  
18 tion systems and organizations).

19 (C) The Green UAS Frameworks of the  
20 Association for Uncrewed Vehicle Systems  
21 International (AUVSI), as amended and ex-  
22 tended.

23 (D) The Cross-Sector Cybersecurity Per-  
24 formance Goals of The Cybersecurity and Infra-  
25 structure Security Agency.

1           (5) CONSULTATION.—In developing the guide-  
2       lines required by paragraph (1), the Under Sec-  
3       retary shall consult with the Administrator of the  
4       Federal Aviation Administration, the Attorney Gen-  
5       eral, and the heads of such other departments and  
6       agencies of the Federal Government as the Under  
7       Secretary considers appropriate.

8       (b) REVIEW OF FEDERAL AGENCY INFORMATION SE-  
9       curity POLICIES AND PRINCIPLES.—

10           (1) REQUIREMENT.—

11           (A) IN GENERAL.—Not later than 1 year  
12       after the date on which the Under Secretary  
13       completes the development of the guidelines re-  
14       quired under subsection (a), the Director shall  
15       require not less than 1 agency, on a pilot basis,  
16       to implement policies and principles based on  
17       the guidelines with respect to unmanned air-  
18       craft systems owned or controlled by the agen-  
19       cy.

20           (B) EXCEPTION.—A pilot implementation  
21       under subparagraph (A) shall not apply to any  
22       unmanned aircraft system comprised of any na-  
23       tional security system.

24           (2) POLICIES AND PRINCIPLES.—Not later than  
25       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-

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

7 (d) REVISION OF FEDERAL ACQUISITION REGULA-  
 8 TION.—The Federal Acquisition Regulation shall be re-  
 9 vised as necessary to implement any standards and guide-  
 10 lines promulgated in this section.

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

14 (a) IN GENERAL.—

15 (1) GUIDANCE.—The Director shall issue guid-  
 16 ance to agencies that includes—

17 (A) requirements for the reporting, coordi-  
 18 nating, and receiving of information about—

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

22 (ii) the resolution of a security vulner-  
 23 ability described in clause (i); and

24 (B) requirements relating to the scope of  
 25 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-

1 half of an agency by the contractor or awardee  
2 contains a security vulnerability, including a  
3 supply chain compromise or an identified soft-  
4 ware or hardware vulnerability, that has been  
5 reported to the contractor or awardee by a third  
6 party, including through a vulnerability disclo-  
7 sure program.

8 (b) REGULATIONS; MODIFICATIONS.—

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

11 (A) the Federal Acquisition Regulatory  
12 Council shall promulgate regulations, as appro-  
13 priate, relating to the responsibilities of con-  
14 tractors and recipients of other transaction  
15 agreements and cooperative agreements to com-  
16 ply with subsection (a)(2); and

17 (B) the Office of Federal Financial Man-  
18 agement shall promulgate regulations under  
19 title 2, Code of Federal Regulations, as appro-  
20 priate, relating to the responsibilities of grant-  
21 ees to comply with subsection (a)(2).

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

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

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

7 (1) provide support to agencies with respect to  
 8 the implementation of the requirements of this sec-  
 9 tion;

10 (2) develop tools, processes, and other mecha-  
 11 nisms determined appropriate to offer agencies capa-  
 12 bilities to implement the requirements of this sec-  
 13 tion; and

14 (3) upon request by an agency, assist the agen-  
 15 cy in the disclosure to vendors of newly identified se-  
 16 curity vulnerabilities in vendor products and serv-  
 17 ices.

18 **SEC. 5. CONTRACTOR COMPLIANCE WITH COORDINATED**  
 19 **DISCLOSURE OF SECURITY**  
 20 **VULNERABILITIES RELATING TO AGENCY UN-**  
 21 **MANNED AIRCRAFT SYSTEMS.**

22 (a) PROHIBITION ON PROCUREMENT AND USE.—

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

1       manned aircraft system if the Chief Information Of-  
2       ficer of the agency determines, in conducting the re-  
3       view required under section 11319(b)(1)(C) of title  
4       40, United States Code, of the contract for the un-  
5       manned aircraft system, that the use of the un-  
6       manned aircraft system prevents compliance with  
7       the standards and guidelines developed under section  
8       3(a)(1) of this Act or the guidelines issued under  
9       section 4(a)(1) of this Act with respect to the un-  
10      manned aircraft system.

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

14           (A) solely from a commercial or nonprofit  
15      entity, the contract or agreement for which does  
16      not specify the type of unmanned aircraft sys-  
17      tem or the specifications for the unmanned air-  
18      craft system;

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

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

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

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

3 (b) WAIVER.—

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

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

11 (B) procuring, obtaining, or using the un-  
12 manned aircraft system is necessary for re-  
13 search, testing, evaluation, or training purposes;  
14 or

15 (C) the unmanned aircraft system is  
16 used—

17 (i) in a manner that does not impli-  
18 cate agency operational or cybersecurity  
19 concerns; or

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

23 (2) AGENCY PROCESS.—The Director shall es-  
24 tablish a standardized process for the Chief Infor-  
25 mation Officer of each agency to follow in deter-

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

3 (c) REPORTS TO CONGRESS.—

4 (1) REPORT.—Not later than 2 years after the  
5 date of enactment of this Act, and every 2 years  
6 thereafter until the date that is 6 years after the  
7 date of enactment of this Act, the Comptroller Gen-  
8 eral of the United States, in consultation with the  
9 heads of other Federal agencies as appropriate, shall  
10 submit to the Committee on Homeland Security and  
11 Governmental Affairs of the Senate, the Committee  
12 on Oversight and Accountability of the House of  
13 Representatives, and the Committee on Homeland  
14 Security of the House of Representatives a report—

15 (A) on the effectiveness of the process es-  
16 tablished under subsection (b)(2);

17 (B) that contains recommended best prac-  
18 tices for the procurement of unmanned aircraft  
19 systems; and

20 (C) that lists—

21 (i) the number and type of each un-  
22 manned aircraft system for which a waiver  
23 under subsection (b)(1) was granted dur-  
24 ing the 2-year period prior to the submis-  
25 sion of the report; and

1 (ii) the legal authority under which  
 2 each such waiver was granted, such as  
 3 whether the waiver was granted pursuant  
 4 to subparagraph (A), (B), or (C) of sub-  
 5 section (b).

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

9 (A) a classified annex that contains the in-  
 10 formation described in paragraph (1)(C); and

11 (B) a committee-use only annex that con-  
 12 tains information described in paragraph (1)(C)  
 13 that is law enforcement sensitive.

14 (d) EFFECTIVE DATE.—The prohibition under sub-  
 15 section (a)(1) shall take effect on the date that is 2 years  
 16 after the date of enactment of this Act.

17 **SEC. 6. GOVERNMENT ACCOUNTABILITY OFFICE REPORT**  
 18 **ON CYBERSECURITY CONSIDERATIONS OF**  
 19 **UNMANNED AIRCRAFT SYSTEMS.**

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

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

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

