I

118TH CONGRESS
2D SESSION

H. R. 8965

To promote the development of certain plans, policies, and standards for managing cybersecurity risks and protecting sensitive technology relating to National Aeronautics and Space Administration spacecraft systems, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

JULY 9, 2024

Mr. FROST (for himself and Mr. BEYER) introduced the following bill; which was referred to the Committee on Science, Space, and Technology

---

A BILL

To promote the development of certain plans, policies, and standards for managing cybersecurity risks and protecting sensitive technology relating to National Aeronautics and Space Administration spacecraft systems, 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 ''Spacecraft Cybersecurity Act''.

SEC. 2. FINDINGS.

Congress finds the following:

(1) Malicious actors have targeted sensitive technology data maintained at certain National Aeronautics and Space Administration (NASA) centers.

(2) A 2019 NASA Inspector General audit reported that potential infiltration into NASA's space flight systems to acquire launch codes and flight trajectories of spacecraft remains a particular concern of NASA's information technology security managers.

(3) The 2011 United States–China Economic and Security Commission's annual report stated that ''at least two U.S. Government satellites have each experienced at least two separate instances of interference apparently consistent with cyber activities against their command and control systems.''.

(4) Space Policy Directive-5 on ''Cybersecurity Principles for Space Systems'' issued guidance that Federal departments and agencies support practices within the Federal Government and across the commercial space industry ''that protect space assets and their supporting infrastructure from cyber threats and ensure continuity of operations.''.

(5) NASA relies on industry contractors and commercial entities to carry out development of its advanced space systems and to provide services such

as transporting NASA crew to and from the International Space Station.

(6) A 2024 Government Accountability Office audit found that NASA lacks a plan and time frames to update its acquisition policies and standards to address cybersecurity controls.

SEC. 3. PLAN AND POLICY REVIEWS.

(a) SENSE OF CONGRESS.—It is the sense of Congress that the Administrator of the National Aeronautics and Space Administration (NASA) should take every action to ensure that robust cybersecurity measures are in place to protect sensitive technology data relating to space systems developed within NASA, at NASA contractors, or under commercial services arrangements.

(b) IN GENERAL.—The Administrator shall ensure that NASA's acquisition policies and standards for space systems and services—

(1) include guidelines and controls for managing cybersecurity risks to such systems and services, consistent with Space Policy Directive-5 on ''Cybersecurity Principles for Space Systems''; and

(2) are updated, as appropriate, to address changing cybersecurity threats to such systems and services.

(c) IMPLEMENTATION PLAN.—Not later than 270 days after the date of the enactment of the Act, the Administrator of NASA shall complete an implementation plan to update NASA's acquisition policies and standards for space systems and services, and incorporate guidelines and controls required to protect against cybersecurity risk and cybersecurity threats to such systems and services. The Administrator shall ensure the participation and input of the Chief Engineer, Chief Information Officer, and the Principal Advisor for Enterprise Protection of NASA in the development of such plan. Such plan shall include the following:

(1) Milestone dates for completing such updates.

(2) A process and frequency for reviewing NASA's cybersecurity policies, procedures, and controls for spacecraft programs to address changing cybersecurity risks and cybersecurity threats to such systems and services.

(3) An estimate of the resources required for carrying out the updates and reviews under paragraphs (1) and (2), respectively.

(d) BRIEFING.—Not later than 30 days after the completion of the implementation plan under subsection (c), the Administrator of NASA shall brief the Committee

on Science, Space, and Technology of the House of Representatives and the Committee on Commerce, Science, and Transportation of the Senate on such plan. Such briefing shall also address how such plan can inform the development of a cybersecurity risk management framework for spacecraft developed or used by NASA in pursuit of its missions that encompasses end-to-end mission systems and operations.

○