I

117TH CONGRESS
1ST SESSION

# H. R. 3608

To amend title 41, United States Code, to require information technology contractors to maintain a vulnerability disclosure policy and program, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

MAY 28, 2021

Mr. LIEU introduced the following bill; which was referred to the Committee on Oversight and Reform

# A BILL

To amend title 41, United States Code, to require information technology contractors to maintain a vulnerability disclosure policy and program, 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 ''Improving Contractor Cybersecurity Act''.

## SEC. 2. VULNERABILITY DISCLOSURE POLICY AND PROGRAM REQUIRED FOR INFORMATION TECHNOLOGY CONTRACTORS.

(a) AMENDMENT.—Chapter 47 of division C of subtitle I of title 41, United States Code, is amended by adding at the end the following new section:

### "§ 4715. Vulnerability disclosure policy and program required

"(a) REQUIREMENTS FOR INFORMATION TECHNOLOGY CONTRACTORS.—The head of an executive agency may not enter into a contract for information technology unless the contractor maintains or does the following:

"(1) A vulnerability disclosure policy for information technology that—

"(A) includes—

"(i) a description of which systems are in scope;

"(ii) the type of information technology testing for each system that is allowed (or specifically not authorized);

"(iii) if a contractor includes systems that host sensitive information in the vulnerability disclosure policy, the contractor shall determine whether to impose restrictions on accessing, copying, transferring, storing, using, and retaining such information, including by—

"(I) prohibiting sensitive information from being saved, stored, transferred, or otherwise accessed after initial discovery;

"(II) directing that sensitive information be viewed only to the extent required to identify a vulnerability and that the information not be retained; or

"(III) limiting use of information obtained from interacting with the systems or services to be explored by the researcher to activities directly related to reporting security vulnerabilities;

"(iv) a description of how an individual may submit a vulnerability report that includes—

"(I) the location of where to send the report, such as a web form or email address;

"(II) a description of the type of information necessary to find and analyze the vulnerability (such as a description, the location, and potential impact of the vulnerability, the technical information needed to reproduce the vulnerability, and any proof of concept); and

"(III) a clear statement—

"(aa) that any individual that submits a vulnerability report may do so anonymously; and

"(bb) on how and whether any incomplete submission is evaluated;

"(v) a commitment from the contractor that the contractor will not pursue civil action for any accidental, good faith violation of the vulnerability disclosure policy;

"(vi) a commitment from the contractor that if an individual acting in accordance with the vulnerability disclosure policy of the contractor is sued by a third party, the contractor will inform the public or the court that the individual was acting in compliance with the vulnerability disclosure policy;

"(vii) a statement that describes the time frame in which the individual that submits a report, if known, will receive a notification of receipt of the report and a description of what steps will be taken by the contractor during the remediation process; and

"(viii) a set of guidelines that establishes what type of activity by a researcher are acceptable and unacceptable; and

"(B) does not—

"(i) require the submission of personally identifiable information of a researcher; and

"(ii) limit testing solely to entities approved by the contractor but rather authorizes the public to search for and report any vulnerability.

"(2) A description of additional procedures that describe how the contractor will communicate with the researcher, and how and when any communication occurs.

“(3) A description of the target timelines for and tracking of the following:

“(A) Notification of receipt to the individual that submits the report, if known.

“(B) An initial assessment, such as determining whether any disclosed vulnerability is valid.

“(C) Resolution of a vulnerability, including notification of the outcome to the researcher.

“(4) A page on the website of the contractor that—

“(A) allows for the submission of vulnerabilities by anyone relating to the information technology;

“(B) lists the contact information, such as a phone number or email address for an individual or team responsible for reviewing any such submission under subparagraph (A); and

“(C) describes the process by which a review is conducted, including how long it will take for the contractor to respond to researcher and whether or not monetary rewards will be paid to the reporter for identifying a vulnerability.

"(5) In the case of a discovered vulnerability that the contractor is not responsible for patching, the contractor shall submit the vulnerability to the responsible party or direct the researcher to the appropriate party.

"(b) REPORTING REQUIREMENTS AND METRICS.—Not later than 7 days after the date on which the vulnerability disclosure policy described in subsection (a) is published, and on an ongoing basis as vulnerability reports are received, an information technology contractor shall report to the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security the following information:

"(1) Any valid or credible report of a not previously known public vulnerability (including any misconfiguration) on a system that uses commercial software or services that affect or are likely to affect other parties in government or industry once a patch or viable mitigation is available.

"(2) Any other situation where the contractor determines it would be helpful or necessary to involve the Cybersecurity and Infrastructure Security Agency.

"(c) CISA SUBMISSION OF VULNERABILITIES.—The Cybersecurity and Infrastructure Security Agency shall communicate with and submit, as necessary, vulnerabilities to the MITRE Common Vulnerabilities and Exposures database and the National Institute of Standards and Technology National Vulnerability Database.

''(d) DEFINITIONS.—In this section:

''(1) EXECUTIVE AGENCY.—The term 'executive agency' has the meaning given that term in section 133.

''(2) RESEARCHER.—The term 'researcher' means the individual who submits a vulnerability report.

''(3) INFORMATION TECHNOLOGY.—The term 'information technology' has the meaning given that term in section 11101 of title 40.''.

(b) TECHNICAL AND CONFORMING AMENDMENT.—The table of sections for chapter 47 of division C of subtitle I of title 41, United States Code, is amended by adding at the end the following new item:

''4715. Vulnerability disclosure policy and program required.''.

(c) APPLICABILITY.—The amendments made by this section shall take effect on the date of the enactment of this section and shall apply to any contract entered into on or after such effective date.

○