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.

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 "Improving Contractor

5 Cybersecurity Act".

SEC. 2. VULNERABILITY DISCLOSURE POLICY AND PRO-GRAM REQUIRED FOR INFORMATION TECH-NOLOGY 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 TECH-NOLOGY 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,

1   storing, using, and retaining such informa-

2   tion, including by—

3   "(I) prohibiting sensitive infor-

4   mation from being saved, stored,

5   transferred, or otherwise accessed

6   after initial discovery;

7   "(II) directing that sensitive in-

8   formation be viewed only to the extent

9   required to identify a vulnerability

10   and that the information not be re-

11   tained; or

12   "(III) limiting use of information

13   obtained from interacting with the

14   systems or services to be explored by

15   the researcher to activities directly re-

16   lated to reporting security

17   vulnerabilities;

18   "(iv) a description of how an indi-

19   vidual may submit a vulnerability report

20   that includes—

21   "(I) the location of where to send

22   the report, such as a web form or

23   email address;

24   "(II) a description of the type of

25   information necessary to find and

1   analyze the vulnerability (such as a

2   description, the location, and potential

3   impact of the vulnerability, the tech-

4   nical information needed to reproduce

5   the vulnerability, and any proof of

6   concept); and

7   "(III) a clear statement—

8   "(aa) that any individual

9   that submits a vulnerability re-

10   port may do so anonymously; and

11   "(bb) on how and whether

12   any incomplete submission is

13   evaluated;

14   "(v) a commitment from the con-

15   tractor that the contractor will not pursue

16   civil action for any accidental, good faith

17   violation of the vulnerability disclosure pol-

18   icy;

19   "(vi) a commitment from the con-

20   tractor that if an individual acting in ac-

21   cordance with the vulnerability disclosure

22   policy of the contractor is sued by a third

23   party, the contractor will inform the public

24   or the court that the individual was acting

1   in compliance with the vulnerability disclo-

2   sure policy;

3   "(vii) a statement that describes the

4   time frame in which the individual that

5   submits a report, if known, will receive a

6   notification of receipt of the report and a

7   description of what steps will be taken by

8   the contractor during the remediation

9   process; and

10   "(viii) a set of guidelines that estab-

11   lishes what type of activity by a researcher

12   are acceptable and unacceptable; and

13   "(B) does not—

14   "(i) require the submission of person-

15   ally identifiable information of a re-

16   searcher; and

17   "(ii) limit testing solely to entities ap-

18   proved by the contractor but rather au-

19   thorizes the public to search for and report

20   any vulnerability.

21   "(2) A description of additional procedures that

22 describe how the contractor will communicate with

23 the researcher, and how and when any communica-

24 tion occurs.

1 ''(3) A description of the target timelines for

2 and tracking of the following:

3   ''(A) Notification of receipt to the indi-

4 vidual that submits the report, if known.

5   ''(B) An initial assessment, such as deter-

6 mining whether any disclosed vulnerability is

7 valid.

8   ''(C) Resolution of a vulnerability, includ-

9 ing notification of the outcome to the re-

10 searcher.

11   ''(4) A page on the website of the contractor

12 that—

13   ''(A) allows for the submission of

14 vulnerabilities by anyone relating to the infor-

15 mation technology;

16   ''(B) lists the contact information, such as

17 a phone number or email address for an indi-

18 vidual or team responsible for reviewing any

19 such submission under subparagraph (A); and

20   ''(C) describes the process by which a re-

21 view is conducted, including how long it will

22 take for the contractor to respond to researcher

23 and whether or not monetary rewards will be

24 paid to the reporter for identifying a vulner-

25 ability.

1 ''(5) In the case of a discovered vulnerability

2 that the contractor is not responsible for patching,

3 the contractor shall submit the vulnerability to the

4 responsible party or direct the researcher to the ap-

5 propriate party.

6 ''(b) REPORTING REQUIREMENTS AND METRICS.—

7 Not later than 7 days after the date on which the vulner-

8 ability disclosure policy described in subsection (a) is pub-

9 lished, and on an ongoing basis as vulnerability reports

10 are received, an information technology contractor shall

11 report to the Cybersecurity and Infrastructure Security

12 Agency of the Department of Homeland Security the fol-

13 lowing information:

14 ''(1) Any valid or credible report of a not pre-

15 viously known public vulnerability (including any

16 misconfiguration) on a system that uses commercial

17 software or services that affect or are likely to affect

18 other parties in government or industry once a patch

19 or viable mitigation is available.

20 ''(2) Any other situation where the contractor

21 determines it would be helpful or necessary to in-

22 volve the Cybersecurity and Infrastructure Security

23 Agency.

24 ''(c) CISA SUBMISSION OF VULNERABILITIES.—The

25 Cybersecurity and Infrastructure Security Agency shall

1 communicate with and submit, as necessary,
2 vulnerabilities to the MITRE Common Vulnerabilities and
3 Exposures database and the National Institute of Stand-
4 ards and Technology National Vulnerability Database.

5 "(d) DEFINITIONS.—In this section:

6 "(1) EXECUTIVE AGENCY.—The term 'executive
7 agency' has the meaning given that term in section
8 133.

9 "(2) RESEARCHER.—The term 'researcher'
10 means the individual who submits a vulnerability re-
11 port.

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

15 (b) TECHNICAL AND CONFORMING AMENDMENT.—
16 The table of sections for chapter 47 of division C of sub-
17 title I of title 41, United States Code, is amended by add-
18 ing at the end the following new item:

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

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

○