

116TH CONGRESS  
2D SESSION

# H. R. 7998

To require the Director of the National Institute of Standards and Technology to disseminate guidance to institutions of higher education and nonprofit research institutions to help mitigate cybersecurity risks to COVID-19 related research, and for other purposes.

---

## IN THE HOUSE OF REPRESENTATIVES

AUGUST 11, 2020

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

---

## A BILL

To require the Director of the National Institute of Standards and Technology to disseminate guidance to institutions of higher education and nonprofit research institutions to help mitigate cybersecurity risks to COVID-19 related research, 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 “NIST COVID–19 Cy-  
5 bersecurity Act”.

6 **SEC. 2. DEFINITIONS.**

7 In this Act:

1           (1) DIRECTOR.—The term “Director” means  
2 the Director of the National Institute of Standards  
3 and Technology.

4           (2) INSTITUTION OF HIGHER EDUCATION.—The  
5 term “institution of higher education” has the  
6 meaning given such term in section 101 of the High-  
7 er Education Act of 1965 (20 U.S.C. 1001).

8           (3) RESOURCES.—The term “resources” means  
9 guidelines, tools, best practices, standards, meth-  
10 odologies, and other ways of providing information.

11           (4) RESEARCH INSTITUTION.—The term “re-  
12 search institution”—

13                 (A) means a nonprofit institution (as de-  
14 fined in section 4(5) of the Stevenson-Wydler  
15 Technology Innovation Act of 1980 (15 U.S.C.  
16 3703(5))); and

17                 (B) includes federally funded research and  
18 development centers, as identified by the Na-  
19 tional Science Foundation in accordance with  
20 the Federal Acquisition Regulation issued in ac-  
21 cordance with section 1303(a)(1) of title 41 (or  
22 any successor regulation).

1 **SEC. 3. IMPROVING CYBERSECURITY OF INSTITUTIONS OF**  
2 **HIGHER EDUCATION.**

3 Section 2(e)(1)(A) of the National Institute of Stand-  
4 ards and Technology Act (15 U.S.C. 272(e)(1)(A)) is  
5 amended—

6 (1) in clause (viii), by striking “and” after the  
7 semicolon;

8 (2) by redesignating clause (ix) as clause (x);  
9 and

10 (3) by inserting after clause (viii) the following:

11 “(ix) consider institutions of higher  
12 education (as defined in section 101 of the  
13 Higher Education Act of 1965 (20 U.S.C.  
14 1001)); and”.

15 **SEC. 4. DISSEMINATION OF RESOURCES FOR RESEARCH IN-**  
16 **STITUTIONS.**

17 (a) IN GENERAL.—Not later than 90 days after the  
18 date of the enactment of this Act, the Director shall, using  
19 the authorities of the Director under subsections (c)(15)  
20 and (e)(1)(A)(ix) of section 2 of the National Institute of  
21 Standards and Technology Act (15 U.S.C. 272), as  
22 amended by section 3, disseminate and make publicly  
23 available resources to help research institutions and insti-  
24 tutions of higher education identify, assess, manage, and  
25 reduce their cybersecurity risk related to conducting re-  
26 search with respect to COVID–19.

1 (b) REQUIREMENTS.—The Director shall ensure that  
2 the resources disseminated pursuant to subsection (a)—

3 (1) are generally applicable and usable by a  
4 wide range of research institutions and institutions  
5 of higher education;

6 (2) vary with the nature and size of the imple-  
7 menting research institutions or institutions of high-  
8 er education, and the nature and sensitivity of the  
9 data collected or stored on the information systems  
10 or devices of the implementing research institutions  
11 or institutions of higher education;

12 (3) include elements that promote awareness of  
13 simple, basic controls, a workplace cybersecurity cul-  
14 ture, and third-party stakeholder relationships, to  
15 assist research institutions or institutions of higher  
16 education in mitigating common cybersecurity risks;

17 (4) include case studies of practical application;

18 (5) are technology-neutral and can be imple-  
19 mented using technologies that are commercial and  
20 off-the-shelf; and

21 (6) to the extent practicable, are based on inter-  
22 national standards.

23 (c) NATIONAL CYBERSECURITY AWARENESS AND  
24 EDUCATION PROGRAM.—The Director shall ensure that  
25 the resources disseminated under subsection (a) are con-

1 sistent with the efforts of the Director under section 401  
2 of the Cybersecurity Enhancement Act of 2014 (15 U.S.C.  
3 7451).

4 (d) UPDATES.—The Director shall review periodically  
5 and update the resources under subsection (a) as the Di-  
6 rector determines appropriate.

7 (e) VOLUNTARY RESOURCES.—The use of the re-  
8 sources disseminated under paragraph (1) shall be consid-  
9 ered voluntary.

10 (f) OTHER FEDERAL CYBERSECURITY REQUIRE-  
11 MENTS.—Nothing in this section may be construed to su-  
12 persede, alter, or otherwise affect any cybersecurity re-  
13 quirements applicable to Federal agencies.

14 (g) FUNDING.—This Act shall be carried out using  
15 funds made available to the Director.

○