

.....
(Original Signature of Member)

119TH CONGRESS
2D SESSION

H. R. _____

To require the Director of the National Institute of Standards and Technology to develop new standards, methodologies, and recommendations with respect to the cybersecurity of cloud-based infrastructure, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

Mr. MCCORMICK introduced the following bill; which was referred to the Committee on _____

A BILL

To require the Director of the National Institute of Standards and Technology to develop new standards, methodologies, and recommendations with respect to the cybersecurity of cloud-based infrastructure, 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 “Common-Sense Cloud
5 Security Act”.

1 **SEC. 2. NATIONAL INSTITUTE OF STANDARDS AND TECH-**
2 **NOLOGY SPECIAL PUBLICATION ON THE CY-**
3 **BERSECURITY OF CLOUD-BASED INFRA-**
4 **STRUCTURE.**

5 (a) IN GENERAL.—Not later than 180 days after the
6 date of the enactment of this Act, the Director of the Na-
7 tional Institute of Standards and Technology (in this sec-
8 tion referred to as the “Director”) shall solicit through
9 the Federal Register public comment on the following:

10 (1) The existing standards, methodologies, and
11 recommendations of the Institute with respect to the
12 cybersecurity of cloud-based infrastructure.

13 (2) Developing new standards, methodologies,
14 and recommendations of the Institute with respect
15 to such cybersecurity, that include the following:

16 (A) Standards for managing and securing
17 the digital identities utilized with respect to
18 such infrastructure, including standards to link
19 logins and other access credentials for an ac-
20 count, which may be an agent account, to a
21 device.

22 (B) Standards for a system through which
23 cloud service providers are able to monitor and
24 address security alerts and unauthorized or ma-
25 licious activity.

1 (C) Recommendations regarding the fol-
2 lowing:

3 (i) Addressing the prevention, detec-
4 tion, and mitigation of intracloud attacks
5 and unauthorized east-west traffic.

6 (ii) Vetting, authorizing, and continu-
7 ously monitoring third-party application in-
8 tegrations and software-as-a-service appli-
9 cations, to ensure that such integrations
10 and applications have appropriate access to
11 the cloud environments of such providers.

12 (iii) Adopting artificial intelligence
13 tools for the detection of unusual or sus-
14 picious activity in such environments, in a
15 manner that resembles such adoption by
16 the Federal Government and other public
17 sector entities.

18 (D) A methodology by which such a pro-
19 vider is able to determine the blast radius of
20 such provider.

21 (b) PROTOTYPE.—Not later than 50 days after the
22 date of the solicitation under subsection (a), the Director
23 shall carry out the following:

24 (1) Publish in the Federal Register a prototype
25 of the standards, methodologies, and recommenda-

1 tions referred to in paragraph (2) of such sub-
2 section.

3 (2) Solicit through the Federal Register public
4 comment on such prototype.

5 (c) FINAL VERSION.—Not later than 135 days after
6 the publication of the prototype of the standards, meth-
7 odologies, and recommendations under subsection (b), the
8 Director shall publish in the Federal Register a final
9 version of such standards, methodologies, and rec-
10 ommendations.

11 (d) CONSULTATION.—In developing the standards,
12 methodologies, and recommendations referred to in para-
13 graph (2) of subsection (a), the Director shall consult with
14 the following:

15 (1) The Secretary of Defense.

16 (2) The National Cyber Director.

17 (3) The Director of the Cybersecurity and In-
18 frastructure Security Agency.

19 (4) Cloud service providers.

20 (5) Owners and operators of critical infrastruc-
21 ture.

22 (6) Associations of entities in critical infrastruc-
23 ture sectors, such as banking and finance and public
24 health and health care.

1 (7) Entities that satisfy the following require-
2 ments (as determined by the Director):

3 (A) Are academic or not-for-profit.

4 (B) Have expertise in cloud security and
5 artificial intelligence governance.

6 (e) CERTIFICATION.—

7 (1) IN GENERAL.—Not later than one year
8 after the publication of the final version of the
9 standards, methodologies, and recommendations
10 under subsection (c), the Director, in coordination
11 with Director of the Cybersecurity and Infrastruc-
12 ture Security Agency, shall establish a program, to
13 be known as the “Cloud Security Certification Pro-
14 gram” (in this section referred to as the “Pro-
15 gram”), that satisfies the following requirements:

16 (A) Is voluntary.

17 (B) Is modeled to the extent practicable on
18 the IT Security Validation Programs of the Na-
19 tional Institute of Standards and Technology,
20 such that third-party, independent, private-sec-
21 tor, accredited testing laboratories conduct eval-
22 uations and make determinations on whether to
23 certify an entity’s conformance with such stand-
24 ards, methodologies, and recommendations, in-
25 cluding with respect to the following:

1 (i) Blast radius.

2 (ii) Intracloud attack.

3 (iii) Third-party application integra-
4 tion.

5 (iv) Workload identity.

6 (C) Includes a public database of each
7 such certification.

8 (D) Includes tiered certification levels.

9 (2) DEADLINE.—Not later than 90 days after
10 the date on which an entity submits to a laboratory
11 under the Program an application for a certification
12 described in subparagraph (B) of paragraph (1),
13 such laboratory shall make for such entity a deter-
14 mination under such subparagraph.

15 (f) FEDERAL RISK AND AUTHORIZATION MANAGE-
16 MENT PROGRAM.—Not later than one year after the publi-
17 cation of the final version of the standards, methodologies,
18 and recommendations under subsection (c), the Director
19 of the Office of Management and Budget, in coordination
20 with the Director of the Cybersecurity and Infrastructure
21 Security Agency and the Administrator of General Serv-
22 ices, shall update the Federal Risk and Authorization
23 Management Program to conform with such standards,
24 methodologies, and recommendations, including by requir-
25 ing each private sector entity that provides cloud services

1 to the Federal Government to disclose to the Director of
2 the Office information relating to the following:

3 (1) The aggregate blast radius of such entity.

4 (2) East-west traffic monitoring, network traf-
5 fic inspection, and policy-based filtering conducted
6 by such entity.

7 (3) The scope and access levels of any third-
8 party application integrations in the cloud environ-
9 ments of such entity.

10 (g) REPORT.—Not later than one year after the pub-
11 lication of the final version of the standards, methodolo-
12 gies, and recommendations under subsection (c), the Di-
13 rector shall submit to the Committee on Science, Space,
14 and Technology of the House of Representatives and the
15 Committee on Commerce, Science, and Transportation of
16 the Senate a report that includes information relating to
17 the following:

18 (1) Implementation by Federal departments
19 and agencies of such standards, methodologies, and
20 recommendations.

21 (2) The gaps and challenges, if any, with re-
22 spect to the adoption of such standards, methodolo-
23 gies, and recommendations by private sector entities.

1 (3) Recommendations of the Director for legis-
2 lative or administrative action with respect to the cy-
3 bersecurity of cloud-based infrastructure.

4 (h) DEFINITIONS.—In this section:

5 (1) ARTIFICIAL INTELLIGENCE.—The term “ar-
6 tificial intelligence” has the meaning given such
7 term in section 5002 of the National Artificial Intel-
8 ligence Initiative Act of 2020 (15 U.S.C. 9401).

9 (2) BLAST RADIUS.—The term “blast radius”
10 means the maximum potential scope of unauthorized
11 data access or system compromise from a com-
12 promised workload, data asset, or credential in a
13 cloud environment.

14 (3) CLOUD-BASED INFRASTRUCTURE.—The
15 term “cloud-based infrastructure” means computing,
16 storage, and networking services, including infra-
17 structure-as-a-service, platform-as-a-service, and
18 software-as-a-service, provided through a public, pri-
19 vate, or hybrid cloud environment.

20 (4) CRITICAL INFRASTRUCTURE.—The term
21 “critical infrastructure” has the meaning given such
22 term in section 1016 of the USA PATRIOT Act (42
23 U.S.C. 5195c).

24 (5) CRITICAL INFRASTRUCTURE SECTORS.—
25 The term “critical infrastructure sectors” has the

1 meaning given such term in section 2001 of the
2 Homeland Security Act of 2002 (6 U.S.C. 601).

3 (6) EAST-WEST TRAFFIC.—The term “east-west
4 traffic” means network traffic between virtual ma-
5 chines, containers, or services in a cloud data center
6 or cloud environment.

7 (7) INTRACLOUD ATTACK.—The term
8 “intracloud attack” means an action by a threat
9 actor to exploit a vulnerability or misconfiguration of
10 a cloud environment and conduct unauthorized lat-
11 eral movement, privilege escalation, or data
12 exfiltration with respect to such environment.

13 (8) NETWORK TRAFFIC INSPECTION.—The
14 term “network traffic inspection” means the moni-
15 toring, examination, and analysis of network com-
16 munications to identify, assess, log, or respond to
17 malicious, unauthorized, or anomalous activity or
18 support the enforcement of a cybersecurity policy.

19 (9) POLICY-BASED FILTERING.—The term “pol-
20 icy-based filtering” means the application of a
21 predefined security policy to permit, deny, restrict,
22 log, or otherwise control network communications
23 based on the source, destination, or content of such
24 communications or an indicator of malicious or un-
25 authorized activity.

1 (10) THIRD-PARTY APPLICATION INTEGRA-
2 TION.—The term “third-party application integra-
3 tion” means the ability of a third party or external
4 software service to interact with a cloud environment
5 through a standardized authorization protocol or ap-
6 plication programming interface.

7 (11) WORKLOAD IDENTITY.—The term “work-
8 load identity” means the digital credentials and to-
9 kens utilized by a nonhuman entity to authenticate
10 or access a cloud resource.