

116TH CONGRESS
2D SESSION

H. R. 7331

To establish the Office of the National Cyber Director, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

JUNE 25, 2020

Mr. LANGEVIN (for himself, Mr. GALLAGHER, Mrs. CAROLYN B. MALONEY of New York, Mr. KATKO, Mr. RUPPERSBERGER, and Mr. HURD of Texas) introduced the following bill; which was referred to the Committee on Oversight and Reform, and in addition to the Committees on Armed Services, Foreign Affairs, and Intelligence (Permanent Select), for a period to be subsequently determined by the Speaker, in each case for consideration of such provisions as fall within the jurisdiction of the committee concerned

A BILL

To establish the Office of the National Cyber Director, 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 “National Cyber Direc-
5 tor Act”.

6 **SEC. 2. NATIONAL CYBER DIRECTOR.**

7 (a) ESTABLISHMENT.—There is established, within
8 the Executive Office of the President, the Office of the

1 National Cyber Director (in this section referred to as the
2 “Office”).

3 (b) NATIONAL CYBER DIRECTOR.—

4 (1) IN GENERAL.—The Office shall be headed
5 by the National Cyber Director (in this section re-
6 ferred to as the “Director”) who shall be appointed
7 by the President, by and with the advice and consent
8 of the Senate. As an exercise of the rulemaking
9 power of the Senate, any nomination of the Director
10 submitted to the Senate for confirmation, and re-
11 ferred to a committee, shall be jointly referred to the
12 Homeland Security and Governmental Affairs and
13 the Armed Services Committees of the Senate. The
14 Director shall hold office at the pleasure of the
15 President, and shall be entitled to receive the same
16 pay and allowances as are provided for level I of the
17 Executive Schedule under section 5312 of title 5,
18 United States Code.

19 (2) DEPUTY DIRECTORS.—There shall be two
20 Deputy National Cyber Directors, to be appointed
21 by the President, who shall hold office at the pleas-
22 ure of the President, and who shall report to the Di-
23 rector, as follows:

24 (A) The Deputy National Cyber Director
25 for Strategy, Capabilities, and Budget.

1 (B) The Deputy National Cyber Director
2 for Plans and Operations.

3 (c) DUTIES OF THE NATIONAL CYBER DIRECTOR.—

4 (1) IN GENERAL.—Subject to the authority, di-
5 rection, and control of the President, the Director
6 shall—

7 (A) serve as the principal advisor to the
8 President on cybersecurity strategy and policy;

9 (B) in consultation with appropriate Fed-
10 eral departments and agencies, develop the
11 United States National Cyber Strategy, which
12 shall include elements related to Federal de-
13 partments and agencies—

14 (i) information security; and

15 (ii) programs and policies intended to
16 improve the United States cybersecurity
17 posture;

18 (C) in consultation with appropriate Fed-
19 eral departments and agencies and upon ap-
20 proval of the National Cyber Strategy by the
21 President, supervise implementation of the
22 strategy by—

23 (i) in consultation with the Director of
24 the Office of Management and Budget,
25 monitoring and assessing the effectiveness,

1 including cost-effectiveness, of Federal de-
2 partments and agencies' implementation of
3 the strategy;

4 (ii) making recommendations relevant
5 to changes in the organization, personnel
6 and resource allocation, and policies of
7 Federal departments and agencies to the
8 Director of the Office of Management and
9 Budget and heads of such departments
10 and agencies in order to implement the
11 strategy;

12 (iii) reviewing the annual budget pro-
13 posal for each Federal department or agen-
14 cy and certifying to the head of each Fed-
15 eral department or agency and the Direc-
16 tor of the Office of Management and
17 Budget whether the department or agency
18 proposal is consistent with the strategy;

19 (iv) continuously assessing and mak-
20 ing relevant recommendations to the Presi-
21 dent on the appropriate level of integration
22 and interoperability across the Federal
23 cybersecurity operations centers;

24 (v) coordinating with the Federal
25 Chief Information Officer, the Federal

1 Chief Information Security Officer, the Di-
2 rector of the Cybersecurity and Infrastruc-
3 ture Security Agency, and the Director of
4 National Institute of Standards and Tech-
5 nology on the development and implemen-
6 tation of policies and guidelines related to
7 issues of Federal department and agency
8 information security; and

9 (vi) reporting annually to the Presi-
10 dent and the Congress on the state of the
11 United States cybersecurity posture, the
12 effectiveness of the strategy, and the sta-
13 tus of Federal departments and agencies’
14 implementation of the strategy;

15 (D) lead joint interagency planning for the
16 Federal Government’s integrated response to
17 cyberattacks and cyber campaigns of significant
18 consequence, to include—

19 (i) coordinating with relevant Federal
20 departments and agencies in the develop-
21 ment of, for the approval of the President,
22 joint, integrated operational plans, proc-
23 esses, and playbooks for incident response
24 that feature—

1 (I) clear lines of authority and
2 lines of effort across the Federal Gov-
3 ernment;

4 (II) authorities that have been
5 delegated to an appropriate level to
6 facilitate effective operational re-
7 sponses across the Federal Govern-
8 ment; and

9 (III) support for the integration
10 of defensive cyber plans and capabili-
11 ties with offensive cyber plans and ca-
12 pabilities in a manner consistent with
13 improving the United States cyberse-
14 curity posture;

15 (ii) exercising these operational plans,
16 processes, and playbooks;

17 (iii) updating these operational plans,
18 processes, and playbooks for incident re-
19 sponse as needed in coordination with on-
20 going offensive cyber plans and operations;
21 and

22 (iv) ensuring these plans, processes,
23 and playbooks are properly coordinated
24 with relevant private sector entities, as ap-
25 propriate;

1 (E) direct the Federal Government's re-
2 sponse to cyberattacks and cyber campaigns of
3 significant consequence, to include—

4 (i) developing for the approval of the
5 President, with the heads of relevant Fed-
6 eral departments and agencies independ-
7 ently or through the National Security
8 Council as directed by the President, oper-
9 ational priorities, requirements, and tasks;

10 (ii) coordinating, deconflicting, and
11 ensuring the execution of operational ac-
12 tivities in incident response; and

13 (iii) coordinating operational activities
14 with relevant private sector entities;

15 (F) engage with private sector leaders on
16 cybersecurity and emerging technology issues
17 with the support of, and in coordination with,
18 the Cybersecurity and Infrastructure Security
19 Agency and other Federal departments and
20 agencies, as appropriate;

21 (G) annually report to Congress on cyber-
22 security threats and issues facing the nation,
23 including any new or emerging technologies
24 that may impact national security, economic
25 prosperity, or enforcing the rule of law; and

1 (H) be responsible for such other functions
2 as the President may direct.

3 (2) DELEGATION OF AUTHORITY.—The Direc-
4 tor may—

5 (A) serve as the senior representative on
6 any body that the President may establish for
7 the purpose of providing the President advice
8 on cybersecurity;

9 (B) be empowered to convene National Se-
10 curity Council, National Economic Council and
11 Homeland Security Council meetings, with the
12 concurrence of the National Security Advisor,
13 Homeland Security Advisor, or Director of the
14 National Economic Council, as appropriate;

15 (C) be included as a participant in prep-
16 arations for and, if appropriate, execution of cy-
17 bersecurity summits and other international
18 meetings at which cybersecurity is a major
19 topic;

20 (D) delegate any of the Director's func-
21 tions, powers, and duties to such officers and
22 employees of the Office as he may designate;
23 and

24 (E) authorize such successive re-delega-
25 tions of such functions, powers, and duties to

1 such officers and employees of the Office as he
2 may deem appropriate.

3 (d) ATTENDANCE AND PARTICIPATION IN NATIONAL
4 SECURITY COUNCIL MEETINGS.—Section 101(c)(2) of the
5 National Security Act of 1947 (50 U.S.C. 3021(c)(2)) is
6 amended by striking “and the Chairman of the Joint
7 Chiefs of Staff” and inserting “the Chairman of the Joint
8 Chiefs of Staff, and the National Cyber Director”.

9 (e) POWERS OF THE DIRECTOR.—The Director may,
10 for the purposes of carrying out the Director’s functions
11 under this section—

12 (1) subject to the civil service and classification
13 laws, select, appoint, employ, and fix the compensa-
14 tion of such officers and employees as are necessary
15 and prescribe their authority and duties, except that
16 not more than 75 individuals may be employed with-
17 out regard to any provision of law regulating the
18 employment or compensation at rates not to exceed
19 the basic rate of basic pay payable for level IV of
20 the Executive Schedule under section 5315 of title
21 5, United States Code;

22 (2) employ experts and consultants in accord-
23 ance with section 3109 of title 5, United States
24 Code, and compensate individuals so employed for
25 each day (including travel time) at rates not in ex-

1 cess of the maximum rate of basic pay for grade
2 GS-15 as provided in section 5332 of such title, and
3 while such experts and consultants are so serving
4 away from their homes or regular place of business,
5 to pay such employees travel expenses and per diem
6 in lieu of subsistence at rates authorized by section
7 5703 of such title 5 for persons in Federal Govern-
8 ment service employed intermittently;

9 (3) promulgate such rules and regulations as
10 may be necessary to carry out the functions, powers,
11 and duties vested in the Director;

12 (4) utilize, with their consent, the services, per-
13 sonnel, and facilities of other Federal agencies;

14 (5) enter into and perform such contracts,
15 leases, cooperative agreements, or other transactions
16 as may be necessary in the conduct of the work of
17 the Office and on such terms as the Director may
18 determine appropriate, with any Federal agency, or
19 with any public or private person or entity;

20 (6) accept voluntary and uncompensated serv-
21 ices, notwithstanding the provisions of section 1342
22 of title 31, United States Code;

23 (7) adopt an official seal, which shall be judi-
24 cially noticed; and

1 (8) provide, where authorized by law, copies of
2 documents to persons at cost, except that any funds
3 so received shall be credited to, and be available for
4 use from, the account from which expenditures relat-
5 ing thereto were made.

6 (f) DEFINITIONS.—In this section:

7 (1) CYBERSECURITY POSTURE.—The term “cy-
8 bersecurity posture” means the ability to identify
9 and protect, and detect, respond to and recover from
10 intrusions in, information systems the compromise of
11 which could constitute a cyber attack or cyber cam-
12 paign of significant consequence.

13 (2) CYBER ATTACKS AND CYBER CAMPAIGNS OF
14 SIGNIFICANT CONSEQUENCE.—The term “cyber at-
15 tacks and cyber campaigns of significant con-
16 sequence” means an incident or series of incidents
17 that have the purpose or effect of—

18 (A) causing a significant disruption to the
19 availability of a Federal information system;

20 (B) harming, or otherwise significantly
21 compromising the provision of service by, a
22 computer or network of computers that support
23 one or more entities in a critical infrastructure
24 sector;

1 (C) significantly compromising the provi-
2 sion of services by one or more entities in a
3 critical infrastructure sector;

4 (D) causing a significant misappropriation
5 of funds or economic resources, trade secrets,
6 personal identifiers, or financial information for
7 commercial or competitive advantage or private
8 financial gain; or

9 (E) otherwise constituting a significant
10 threat to the national security, foreign policy, or
11 economic health or financial stability of the
12 United States.

13 (3) INCIDENT.—The term “incident” has the
14 meaning given that term in section 3552 of title 44,
15 United States Code.

16 (4) INFORMATION SECURITY.—The term “infor-
17 mation security” has the meaning given that term in
18 section 3552 of title 44, United States Code.

○