

(2) Excepted service

The term “excepted service” has the meaning given that term in section 2103 of title 5.

(3) Historically Black college or university

The term “historically Black college or university” has the meaning given the term “part B institution” in section 1061 of title 20.

(4) Institution of higher education

The term “institution of higher education” has the meaning given that term in section 1001 of title 20.

(5) Minority-serving institution

The term “minority-serving institution” means an institution of higher education described in section 1067q(a) of title 20.

(b) Program

The Secretary shall carry out an intelligence and cybersecurity diversity fellowship program (in this section referred to as the “Program”) under which an eligible individual may—

(1) participate in a paid internship at the Department that relates to intelligence, cybersecurity, or some combination thereof;

(2) receive tuition assistance from the Secretary; and

(3) upon graduation from an institution of higher education and successful completion of the Program (as defined by the Secretary), receive an offer of employment to work in an intelligence or cybersecurity position of the Department that is in the excepted service.

(c) Eligibility

To be eligible to participate in the Program, an individual shall—

(1) be a citizen of the United States; and

(2) as of the date of submitting the application to participate in the Program—

(A) have a cumulative grade point average of at least 3.2 on a 4.0 scale;

(B) be a socially disadvantaged individual (as that term in¹ defined in section 124.103 of title 13, Code of Federal Regulations, or successor regulation); and

(C) be a sophomore, junior, or senior at an institution of higher education.

(d) Direct hire authority

If an individual who receives an offer of employment under subsection (b)(3) accepts such offer, the Secretary shall appoint, without regard to provisions of subchapter I of chapter 33 of title 5 (except for section 3328 of such title) such individual to the position specified in such offer.

(e) Reports**(1) Reports**

Not later than 1 year after December 27, 2020, and on an annual basis thereafter, the Secretary shall submit to the appropriate committees of Congress a report on the Program.

(2) Matters

Each report under paragraph (1) shall include, with respect to the most recent year, the following:

(A) A description of outreach efforts by the Secretary to raise awareness of the Program among institutions of higher education in which eligible individuals are enrolled.

(B) Information on specific recruiting efforts conducted by the Secretary to increase participation in the Program.

(C) The number of individuals participating in the Program, listed by the institution of higher education in which the individual is enrolled at the time of participation, and information on the nature of such participation, including on whether the duties of the individual under the Program relate primarily to intelligence or to cybersecurity.

(D) The number of individuals who accepted an offer of employment under the Program and an identification of the element within the Department to which each individual was appointed.

(Pub. L. 107-296, title XIII, §1333, as added Pub. L. 116-260, div. W, title IV, §404(a), Dec. 27, 2020, 134 Stat. 2378.)

Editorial Notes**CODIFICATION**

Section was enacted as part of title XIII of Pub. L. 107-296, and not as part of title XXII of 107-296 which comprises this subchapter.

§ 665b. Joint cyber planning office**(a) Establishment of Office**

There is established in the Agency an office for joint cyber planning (in this section referred to as the “Office”) to develop, for public and private sector entities, plans for cyber defense operations, including the development of a set of coordinated actions to protect, detect, respond to, and recover from cybersecurity risks or incidents or limit, mitigate, or defend against coordinated, malicious cyber operations that pose a potential risk to critical infrastructure or national interests. The Office shall be headed by a senior official of the Agency selected by the Director.

(b) Planning and execution

In leading the development of plans for cyber defense operations pursuant to subsection (a), the head of the Office shall—

(1) coordinate with relevant Federal departments and agencies to establish processes and procedures necessary to develop and maintain ongoing coordinated plans for cyber defense operations;

(2) leverage cyber capabilities and authorities of participating Federal departments and agencies, as appropriate, in furtherance of plans for cyber defense operations;

(3) ensure that plans for cyber defense operations are, to the greatest extent practicable, developed in collaboration with relevant private sector entities, particularly in areas in which such entities have comparative advantages in limiting, mitigating, or defending against a cybersecurity risk or incident or coordinated, malicious cyber operation;

(4) ensure that plans for cyber defense operations, as appropriate, are responsive to po-

¹ So in original. Probably should be “is”.

tential adversary activity conducted in response to United States offensive cyber operations;

(5) facilitate the exercise of plans for cyber defense operations, including by developing and modeling scenarios based on an understanding of adversary threats to, vulnerability of, and potential consequences of disruption or compromise of critical infrastructure;

(6) coordinate with and, as necessary, support relevant Federal departments and agencies in the establishment of procedures, development of additional plans, including for offensive and intelligence activities in support of cyber defense operations, and creation of agreements necessary for the rapid execution of plans for cyber defense operations when a cybersecurity risk or incident or malicious cyber operation has been identified; and

(7) support public and private sector entities, as appropriate, in the execution of plans developed pursuant to this section.

(c) Composition

The Office shall be composed of—

- (1) a central planning staff; and
- (2) appropriate representatives of Federal departments and agencies, including—
 - (A) the Department;
 - (B) United States Cyber Command;
 - (C) the National Security Agency;
 - (D) the Federal Bureau of Investigation;
 - (E) the Department of Justice; and
 - (F) the Office of the Director of National Intelligence.

(d) Consultation

In carrying out its responsibilities described in subsection (b), the Office shall regularly consult with appropriate representatives of non-Federal entities, such as—

- (1) State, local, federally-recognized Tribal, and territorial governments;
- (2) Information Sharing and Analysis Organizations, including information sharing and analysis centers;
- (3) owners and operators of critical information systems;
- (4) private entities; and
- (5) other appropriate representatives or entities, as determined by the Secretary.

(e) Interagency agreements

The Secretary and the head of a Federal department or agency referred to in subsection (c) may enter into agreements for the purpose of detailing personnel on a reimbursable or non-reimbursable basis.

(f) Definitions

In this section, the term “cyber defense operation” means the defensive activities performed for a cybersecurity purpose.

(Pub. L. 107–296, title XXII, § 2216, formerly § 2215, as added Pub. L. 116–283, div. A, title XVII, § 1715(a), Jan. 1, 2021, 134 Stat. 4092; renumbered § 2216 and amended Pub. L. 117–81, div. A, title XV, § 1547(b)(1)(A)(iii), Dec. 27, 2021, 135 Stat. 2061; Pub. L. 117–263, div. G, title LXXI, § 7143(b)(2)(I), Dec. 23, 2022, 136 Stat. 3660.)

Editorial Notes

PRIOR PROVISIONS

A prior section 2216 of Pub. L. 107–296 was renumbered section 2219 and is classified to section 665e of this title.

AMENDMENTS

2022—Subsec. (d)(2). Pub. L. 117–263, § 7143(b)(2)(I)(i), substituted “Information Sharing and Analysis Organizations” for “information sharing and analysis organizations”.

Subsec. (f). Pub. L. 117–263, § 7143(b)(2)(I)(ii), substituted “section, the term ‘cyber defense operation’ means the defensive activities performed for a cybersecurity purpose.” for “section:” and struck out pars. (1) to (4) which defined cyber defense operation, cybersecurity purpose, cybersecurity risk, incident, and information sharing and analysis organization.

2021—Pub. L. 117–81 reenacted section catchline.

§ 665c. Cybersecurity State Coordinator

(a) Appointment

The Director shall appoint an employee of the Agency in each State, with the appropriate cybersecurity qualifications and expertise, who shall serve as the Cybersecurity State Coordinator.

(b) Duties

The duties of a Cybersecurity State Coordinator appointed under subsection (a) shall include—

(1) building strategic public and, on a voluntary basis, private sector relationships, including by advising on establishing governance structures to facilitate the development and maintenance of secure and resilient infrastructure;

(2) serving as the Federal cybersecurity risk advisor and supporting preparation, response, and remediation efforts relating to cybersecurity risks and incidents;

(3) facilitating the sharing of cyber threat information to improve understanding of cybersecurity risks and situational awareness of cybersecurity incidents;

(4) raising awareness of the financial, technical, and operational resources available from the Federal Government to non-Federal entities to increase resilience against cyber threats;

(5) supporting training, exercises, and planning for continuity of operations to expedite recovery from cybersecurity incidents, including ransomware;

(6) serving as a principal point of contact for non-Federal entities to engage, on a voluntary basis, with the Federal Government on preparing, managing, and responding to cybersecurity incidents;

(7) assisting non-Federal entities in developing and coordinating vulnerability disclosure programs consistent with Federal and information security industry standards;

(8) assisting State, local, Tribal, and territorial governments, on a voluntary basis, in the development of State cybersecurity plans;

(9) coordinating with appropriate officials within the Agency; and

(10) performing such other duties as determined necessary by the Director to achieve the goal of managing cybersecurity risks in