

“(4) The term ‘eligible individual, organization, or company’ means an individual, organization, or company that meets such criteria as the Secretary determines in order to receive compensation in compliance with Federal laws.

“(5) The term ‘information system’ has the meaning given the term in section 3502 of title 44, United States Code.

“(6) The term ‘pilot program’ means the bug bounty pilot program required to be established under subsection (b)(1).

“(7) The term ‘Secretary’ means the Secretary of Homeland Security.

“(b) BUG BOUNTY PILOT PROGRAM.—

“(1) ESTABLISHMENT.—Not later than 180 days after the date of enactment of this Act [Dec. 21, 2018], the Secretary shall establish, within the Office of the Chief Information Officer, a bug bounty pilot program to minimize vulnerabilities of appropriate information systems of the Department.

“(2) RESPONSIBILITIES OF SECRETARY.—In establishing and conducting the pilot program, the Secretary shall—

“(A) designate appropriate information systems to be included in the pilot program;

“(B) provide compensation to eligible individuals, organizations, and companies for reports of previously unidentified security vulnerabilities within the information systems designated under subparagraph (A);

“(C) establish criteria for individuals, organizations, and companies to be considered eligible for compensation under the pilot program in compliance with Federal laws;

“(D) consult with the Attorney General on how to ensure that approved individuals, organizations, or companies that comply with the requirements of the pilot program are protected from prosecution under section 1030 of title 18, United States Code, and similar provisions of law, and civil lawsuits for specific activities authorized under the pilot program;

“(E) consult with the Secretary of Defense and the heads of other departments and agencies that have implemented programs to provide compensation for reports of previously undisclosed vulnerabilities in information systems, regarding lessons that may be applied from such programs; and

“(F) develop an expeditious process by which an individual, organization, or company can register with the Department, submit to a background check as determined by the Department, and receive a determination as to eligibility; and

“(G) engage qualified interested persons, including non-government sector representatives, about the structure of the pilot program as constructive and to the extent practicable.

“(3) CONTRACT AUTHORITY.—In establishing the pilot program, the Secretary, subject to the availability of appropriations, may award 1 or more competitive contracts to an entity, as necessary, to manage the pilot program.

“(c) REPORT TO CONGRESS.—Not later than 180 days after the date on which the pilot program is completed, the Secretary shall submit to the appropriate congressional committees a report on the pilot program, which shall include—

“(1) the number of individuals, organizations, or companies that participated in the pilot program, broken down by the number of individuals, organizations, or companies that—

“(A) registered;

“(B) were determined eligible;

“(C) submitted security vulnerabilities; and

“(D) received compensation;

“(2) the number and severity of vulnerabilities reported as part of the pilot program;

“(3) the number of previously unidentified security vulnerabilities remediated as a result of the pilot program;

“(4) the current number of outstanding previously unidentified security vulnerabilities and Department remediation plans;

“(5) the average length of time between the reporting of security vulnerabilities and remediation of the vulnerabilities;

“(6) the types of compensation provided under the pilot program; and

“(7) the lessons learned from the pilot program.

“(d) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to be appropriated to the Department \$250,000 for fiscal year 2019 to carry out this section.”

#### AGENCY RESPONSIBILITIES

Pub. L. 114–113, div. N, title II, §223(b), Dec. 18, 2015, 129 Stat. 2966, as amended by Pub. L. 115–278, §2(h)(1)(E), Nov. 16, 2018, 132 Stat. 4182, provided that:

“(1) IN GENERAL.—Except as provided in paragraph (2)—

“(A) not later than 1 year after the date of enactment of this Act [Dec. 18, 2015] or 2 months after the date on which the Secretary makes available the intrusion detection and prevention capabilities under section 2213(b)(1) of the Homeland Security Act of 2002 [6 U.S.C. 663(b)(1)], whichever is later, the head of each agency shall apply and continue to utilize the capabilities to all information traveling between an agency information system and any information system other than an agency information system; and

“(B) not later than 6 months after the date on which the Secretary makes available improvements to the intrusion detection and prevention capabilities pursuant to section 2213(b)(2) of the Homeland Security Act of 2002 [6 U.S.C. 663(b)(2)], the head of each agency shall apply and continue to utilize the improved intrusion detection and prevention capabilities.

“(2) EXCEPTION.—The requirements under paragraph (1) shall not apply to the Department of Defense, a national security system, or an element of the intelligence community.

“(3) DEFINITION.—Notwithstanding section 222 [6 U.S.C. 1521], in this subsection, the term ‘agency information system’ means an information system owned or operated by an agency.

“(4) RULE OF CONSTRUCTION.—Nothing in this subsection shall be construed to limit an agency from applying the intrusion detection and prevention capabilities to an information system other than an agency information system under section 2213(b)(1) of the Homeland Security Act of 2002 [6 U.S.C. 663(b)(1)], at the discretion of the head of the agency or as provided in relevant policies, directives, and guidelines.”

#### § 664. National asset database

##### (a) Establishment

###### (1) National asset database

The Secretary shall establish and maintain a national database of each system or asset that—

(A) the Secretary, in consultation with appropriate homeland security officials of the States, determines to be vital and the loss, interruption, incapacity, or destruction of which would have a negative or debilitating effect on the economic security, public health, or safety of the United States, any State, or any local government; or

(B) the Secretary determines is appropriate for inclusion in the database.

###### (2) Prioritized critical infrastructure list

In accordance with Homeland Security Presidential Directive–7, as in effect on January 1, 2007, the Secretary shall establish and maintain a single classified prioritized list of sys-

terms and assets included in the database under paragraph (1) that the Secretary determines would, if destroyed or disrupted, cause national or regional catastrophic effects.

**(b) Use of database**

The Secretary shall use the database established under subsection (a)(1) in the development and implementation of Department plans and programs as appropriate.

**(c) Maintenance of database**

**(1) In general**

The Secretary shall maintain and annually update the database established under subsection (a)(1) and the list established under subsection (a)(2), including—

(A) establishing data collection guidelines and providing such guidelines to the appropriate homeland security official of each State;

(B) regularly reviewing the guidelines established under subparagraph (A), including by consulting with the appropriate homeland security officials of States, to solicit feedback about the guidelines, as appropriate;

(C) after providing the homeland security official of a State with the guidelines under subparagraph (A), allowing the official a reasonable amount of time to submit to the Secretary any data submissions recommended by the official for inclusion in the database established under subsection (a)(1);

(D) examining the contents and identifying any submissions made by such an official that are described incorrectly or that do not meet the guidelines established under subparagraph (A); and

(E) providing to the appropriate homeland security official of each relevant State a list of submissions identified under subparagraph (D) for review and possible correction before the Secretary finalizes the decision of which submissions will be included in the database established under subsection (a)(1).

**(2) Organization of information in database**

The Secretary shall organize the contents of the database established under subsection (a)(1) and the list established under subsection (a)(2) as the Secretary determines is appropriate. Any organizational structure of such contents shall include the categorization of the contents—

(A) according to the sectors listed in National Infrastructure Protection Plan developed pursuant to Homeland Security Presidential Directive-7; and

(B) by the State and county of their location.

**(3) Private sector integration**

The Secretary shall identify and evaluate methods, including the Department's Protected Critical Infrastructure Information Program, to acquire relevant private sector information for the purpose of using that information to generate any database or list, including the database established under subsection (a)(1) and the list established under subsection (a)(2).

**(4) Retention of classification**

The classification of information required to be provided to Congress, the Department, or any other department or agency under this section by a Sector Risk Management Agency, including the assignment of a level of classification of such information, shall be binding on Congress, the Department, and that other Federal agency.

**(d) Reports**

**(1) Report required**

Not later than 180 days after August 3, 2007, and annually thereafter, the Secretary shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives a report on the database established under subsection (a)(1) and the list established under subsection (a)(2).

**(2) Contents of report**

Each such report shall include the following:

(A) The name, location, and sector classification of each of the systems and assets on the list established under subsection (a)(2).

(B) The name, location, and sector classification of each of the systems and assets on such list that are determined by the Secretary to be most at risk to terrorism.

(C) Any significant challenges in compiling the list of the systems and assets included on such list or in the database established under subsection (a)(1).

(D) Any significant changes from the preceding report in the systems and assets included on such list or in such database.

(E) If appropriate, the extent to which such database and such list have been used, individually or jointly, for allocating funds by the Federal Government to prevent, reduce, mitigate, or respond to acts of terrorism.

(F) The amount of coordination between the Department and the private sector, through any entity of the Department that meets with representatives of private sector industries for purposes of such coordination, for the purpose of ensuring the accuracy of such database and such list.

(G) Any other information the Secretary deems relevant.

**(3) Classified information**

The report shall be submitted in unclassified form but may contain a classified annex.

**(e) National Infrastructure Protection Consortium**

The Secretary may establish a consortium to be known as the "National Infrastructure Protection Consortium". The Consortium may advise the Secretary on the best way to identify, generate, organize, and maintain any database or list of systems and assets established by the Secretary, including the database established under subsection (a)(1) and the list established under subsection (a)(2). If the Secretary establishes the National Infrastructure Protection Consortium, the Consortium may—

(1) be composed of national laboratories, Federal agencies, State and local homeland se-

curity organizations, academic institutions, or national Centers of Excellence that have demonstrated experience working with and identifying critical infrastructure and key resources; and

(2) provide input to the Secretary on any request pertaining to the contents of such database or such list.

(Pub. L. 107–296, title XXII, § 2214, formerly title II, § 210E, as added Pub. L. 110–53, title X, § 1001(a), Aug. 3, 2007, 121 Stat. 372; renumbered title XXII, § 2214, and amended Pub. L. 115–278, § 2(g)(2)(G), (9)(A)(viii), Nov. 16, 2018, 132 Stat. 4178, 4181; Pub. L. 116–283, div. H, title XC, § 9002(c)(2)(E), Jan. 1, 2021, 134 Stat. 4773.)

#### Editorial Notes

##### CODIFICATION

Section was formerly classified to section 124I of this title prior to renumbering by Pub. L. 115–278.

##### AMENDMENTS

2021—Subsec. (c)(4). Pub. L. 116–283 substituted “Sector Risk Management Agency” for “sector-specific agency”.

2018—Subsecs. (e), (f). Pub. L. 115–278, § 2(g)(9)(A)(viii), redesignated subsec. (f) as (e) and struck out former subsec. (e). Prior to amendment, text of subsec. (e) read as follows: “By not later than two years after August 3, 2007, the Inspector General of the Department shall conduct a study of the implementation of this section.”

#### § 665. Duties and authorities relating to .gov internet domain

##### (a) Definition

In this section, the term “agency” has the meaning given the term in section 3502 of title 44.

##### (b) Availability of .gov internet domain

The Director shall make .gov internet domain name registration services, as well as any supporting services described in subsection (e), generally available—

(1) to any Federal, State, local, or territorial government entity, or other publicly controlled entity, including any Tribal government recognized by the Federal Government or a State government, that complies with the requirements for registration developed by the Director as described in subsection (c);

(2) without conditioning registration on the sharing of any information with the Director or any other Federal entity, other than the information required to meet the requirements described in subsection (c); and

(3) without conditioning registration on participation in any separate service offered by the Director or any other Federal entity.

##### (c) Requirements

The Director, with the approval of the Director of the Office of Management and Budget for agency .gov internet domain requirements and in consultation with the Director of the Office of Management and Budget for .gov internet domain requirements for entities that are not agencies, shall establish and publish on a publicly available website requirements for the registration and operation of .gov internet domains sufficient to—

(1) minimize the risk of .gov internet domains whose names could mislead or confuse users;

(2) establish that .gov internet domains may not be used for commercial or political campaign purposes;

(3) ensure that domains are registered and maintained only by authorized individuals; and

(4) limit the sharing or use of any information obtained through the administration of the .gov internet domain with any other Department component or any other agency for any purpose other than the administration of the .gov internet domain, the services described in subsection (e), and the requirements for establishing a .gov inventory described in subsection (h).

#### (d) Executive branch

##### (1) In general

The Director of the Office of Management and Budget shall establish applicable processes and guidelines for the registration and acceptable use of .gov internet domains by agencies.

##### (2) Approval required

The Director shall obtain the approval of the Director of the Office of Management and Budget before registering a .gov internet domain name for an agency.

##### (3) Compliance

Each agency shall ensure that any website or digital service of the agency that uses a .gov internet domain is in compliance with the 21st Century IDEA Act (44 U.S.C. 3501 note) and implementation guidance issued pursuant to that Act.

#### (e) Supporting services

##### (1) In general

The Director may provide services to the entities described in subsection (b)(1) specifically intended to support the security, privacy, reliability, accessibility, and speed of registered .gov internet domains.

##### (2) Rule of construction

Nothing in paragraph (1) shall be construed to—

(A) limit other authorities of the Director to provide services or technical assistance to an entity described in subsection (b)(1); or

(B) establish new authority for services other than those the purpose of which expressly supports the operation of .gov internet domains and the needs of .gov internet domain registrants.

#### (f) Fees

##### (1) In general

The Director may provide any service relating to the availability of the .gov internet domain program, including .gov internet domain name registration services described in subsection (b) and supporting services described in subsection (e), to entities described in subsection (b)(1) with or without reimbursement, including variable pricing.

##### (2) Limitation

The total fees collected for new .gov internet domain registrants or annual renewals of .gov