

.....
(Original Signature of Member)

113TH CONGRESS
2D SESSION

H. R.

To improve the information security of the Department of Veterans Affairs by directing the Secretary of Veterans Affairs to carry out certain actions to improve the transparency and the governance of the information security program of the Department, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

Mrs. WALORSKI introduced the following bill; which was referred to the Committee on _____

A BILL

To improve the information security of the Department of Veterans Affairs by directing the Secretary of Veterans Affairs to carry out certain actions to improve the transparency and the governance of the information security program of the Department, 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; TABLE OF CONTENTS.**

4 (a) SHORT TITLE.—This Act may be cited as the
5 “Veterans Information Security Improvement Act”.

1 (b) TABLE OF CONTENTS.—The table of contents for
2 this Act is as follows:

- Sec. 1. Short title; table of contents.
- Sec. 2. Governance of information security program of Department of Veterans Affairs.
- Sec. 3. Security of critical network infrastructure, including domain controller, of Department of Veterans Affairs.
- Sec. 4. Security of computers and servers of Department of Veterans Affairs.
- Sec. 5. Upgrade or phase-out of unsupported or outdated operating systems.
- Sec. 6. Security of web applications from vital vulnerabilities.
- Sec. 7. Security of the Vista system.
- Sec. 8. Report on compliance with information security requirements and best practices.
- Sec. 9. Reports on implementation.
- Sec. 10. Application.
- Sec. 11. Definitions.

3 **SEC. 2. GOVERNANCE OF INFORMATION SECURITY PRO-**
4 **GRAM OF DEPARTMENT OF VETERANS AF-**
5 **FAIRS.**

6 (a) REQUIREMENTS FOR CERTAIN OFFICIALS AND
7 STAFF.—

8 (1) IN GENERAL.—Subchapter III of chapter
9 57 of title 38, United States Code, is amended by
10 inserting after section 5723 the following new sec-
11 tion:

12 **“§ 5723A. Governance of information security pro-**
13 **gram**

14 “(a) IN GENERAL.—The Secretary shall carry out
15 this section to improve the transparency and the coordina-
16 tion of the information security program of the Depart-
17 ment.

18 “(b) OFFICE OF INFORMATION AND TECHNOLOGY.—

19 (1) The Secretary shall ensure that the Assistant Sec-

1 retary for Information and Technology, as the Chief Infor-
2 mation Officer of the Department, possesses—

3 “(A) the appropriate education and at least 10
4 concurrent years of validated experience and capa-
5 bilities in the management of information technology
6 organizations;

7 “(B) an industry recognized certification in in-
8 formation security and cyber security defense; and

9 “(C) demonstrated, sound technical capabilities.

10 “(2) The Secretary shall ensure that the staff of the
11 Office of Information and Technology who perform secu-
12 rity functions, including the assessment and analysis of
13 risk, security auditing, security operations, and security
14 engineering, are assigned to the Office of Information Se-
15 curity.

16 “(3) The Secretary shall ensure that subordinate of-
17 fices of the Office of Information and Technology, in co-
18 ordination with the head of the Office of Information Se-
19 curity, maintain appropriate information security func-
20 tions within each such office to—

21 “(A) incorporate secure software assurance
22 processes into the software development lifecycle for
23 all software development activities;

24 “(B) validate that each third-party developed
25 software used in any information system of the De-

1 partment meets the standards of the National Insti-
2 tute of Standards and Technology with respect to
3 security, safety, reliability, functionality and extensi-
4 bility;

5 “(C) maintain established information security
6 baseline controls for such information systems, and
7 immediately remediate systems determined to be out
8 of compliance with established baseline controls to
9 the maximum extent possible;

10 “(D) ensure that the security architecture of
11 the Department is documented and fully integrated
12 into the overall enterprise architecture strategy of
13 the Department; and

14 “(E) develop and implement a policy that re-
15 stricts the development of new data warehouses and
16 data marts holding sensitive personal information of
17 veterans and reduces the number of data marts
18 holding such information.

19 “(c) OFFICE OF INFORMATION SECURITY.—(1) The
20 Secretary shall ensure that the head of the Office of Infor-
21 mation Security possesses—

22 “(A) the appropriate education and at least 10
23 concurrent years of experience with respect to vali-
24 dated information security; and

1 “(B) an industry recognized certification in
2 cyber security defense;

3 “(C) demonstrated, sound technical capabilities;
4 and

5 “(D) other relevant experience.

6 “(2) The Secretary shall ensure that all of the field
7 staff of the Office of Information Security, including rel-
8 evant staff of the Office of Information Technology, whose
9 primary responsibility is the protection of personally iden-
10 tifiable information of veterans maintain current informa-
11 tion security training and possess a certain level of infor-
12 mation security, cyber security defense, and technical ca-
13 pabilities and certifications as appropriate.”.

14 (2) CLERICAL AMENDMENT.—The table of sec-
15 tions at the beginning of such chapter is amended
16 by inserting after the item relating to section 5723
17 the following new item:

 “5723A. Governance of information security program.”.

18 (b) DEFINITIONS.—Section 5721 of title 38, United
19 States Code, is amended by adding at the end the fol-
20 lowing new paragraphs:

21 “(24) DATA MART.—The term ‘data mart’
22 means a subset of a data warehouse that contains
23 information for a specific department or entity of an
24 organization rather than the entire organization.

1 “(25) DATA WAREHOUSE.—The term ‘data
2 warehouse’ means a collection of data designed to
3 support management decision making that contains
4 a wide variety of data that present a coherent pic-
5 ture of business conditions for an entire organization
6 at a single point in time and whose development in-
7 cludes the development of systems to extract data
8 from operating systems plus installation of a ware-
9 house database system that provides managers flexi-
10 ble access to the data.”.

11 **SEC. 3. SECURITY OF CRITICAL NETWORK INFRASTRUC-**
12 **TURE, INCLUDING DOMAIN CONTROLLER, OF**
13 **DEPARTMENT OF VETERANS AFFAIRS.**

14 (a) IN GENERAL.—Not later than 90 days after the
15 date of the enactment of this Act, the Secretary of Vet-
16 erans Affairs shall ensure the security and safeguard of
17 the network infrastructure of the Department of Veterans
18 Affairs.

19 (b) ACTIONS REQUIRED.—In carrying out subsection
20 (a), the Secretary shall carry out the following actions:

21 (1) Maintain the awareness and complete phys-
22 ical and logical control of the critical network infra-
23 structure, including routers, switches, domain nam-
24 ing systems, firewalls, load balancers, proxy devices,
25 authentication services, telecommunications, domain

1 controllers, and any device that is part of the trust-
2 ed Internet connection system.

3 (2) If the Secretary determines that any critical
4 network infrastructure device or service has been
5 compromised, restore the device or service to the last
6 known noncompromised state and determine the
7 cause of the compromise.

8 (3) If the Secretary determines that com-
9 promised devices or services must be used for a lim-
10 ited time, conduct such use in accordance with the
11 guidance established by the National Security Agen-
12 cy under the document titled “Information Assur-
13 ance Guidance for Operating on a Compromised
14 Network”, or successor document.

15 (4) Provide special security configurations for
16 protecting critical infrastructure devices and serv-
17 ices.

18 (5) Implement policies and security measures
19 that minimize the threats to critical infrastructure
20 devices and services.

21 (6) Ensure that critical infrastructure devices
22 and services, including the domain controller set-
23 tings, are in compliance with the Server Security
24 Plan of the Department under the Department of
25 Veterans Affairs Handbook 6500.

1 (7) Establish access rights, permissions, and
2 multifactor authentication for the critical infrastruc-
3 ture devices and services, including the domain con-
4 troller, for specific users or groups of users.

5 (8) Ensure that proper physical security meas-
6 ures are taken to safeguard the critical infrastruc-
7 ture devices and services and limit physical access to
8 such location to a limited number of authorized indi-
9 viduals.

10 (9) Limit the access from network connections
11 to critical infrastructure devices and services and
12 only configure services and software that are needed
13 by the devices and services.

14 (10) Disable or delete any service or software
15 from critical infrastructure devices and services that
16 is unnecessary.

17 (11) Where feasible, secure critical infrastruc-
18 ture devices and services with host-based and
19 networked-based security controls and limit the
20 number of ports that are opened between critical in-
21 frastructure devices and services, including any de-
22 vice requesting access to network resources and serv-
23 ices.

1 (12) Conduct regular audits and testing of the
2 backups and restore events of the critical infrastruc-
3 ture devices and services.

4 (13) Ensure that for any device to access and
5 communicate with critical infrastructure devices and
6 services within the domain, the authentication traffic
7 has to be signed and encrypted.

8 (14) Limit the administrator account from ac-
9 cessing critical infrastructure devices and services,
10 including domain controllers, throughout the net-
11 work and use such account only for emergencies.

12 (15) Restrict remote access to local adminis-
13 trator accounts and use firewall rules to restrict lat-
14 eral movement on the network.

15 (16) Conduct regular formal penetration testing
16 to test for potential security weaknesses and resolve
17 such weaknesses by not later than seven days after
18 identifying such weaknesses.

19 (c) CERTIFICATION.—Not later than 30 days after
20 the date of the enactment of this Act, the Secretary shall
21 submit to the congressional veterans committees written
22 certification that the Secretary has commenced each ac-
23 tion described in subsection (b).

1 **SEC. 4. SECURITY OF COMPUTERS AND SERVERS OF DE-**
2 **PARTMENT OF VETERANS AFFAIRS.**

3 (a) IN GENERAL.—The Secretary shall ensure the se-
4 curity of each general purpose computer and server of the
5 Department.

6 (b) ACTIONS REQUIRED.—In carrying out subsection
7 (a), the Secretary shall carry out the following actions:

8 (1) Formalize and enforce a Department-wide
9 process to monitor software installed on general pur-
10 pose computers and servers of the Department, pre-
11 vent the unauthorized installation of software, and
12 remove any unauthorized software that has been in-
13 stalled.

14 (2) Not later than 45 days after the date of the
15 enactment of this Act, implement automated
16 patching tools and processes that ensure that secu-
17 rity patches are installed for any software or oper-
18 ating system on a computer by not later than 48
19 hours after the patch is made available.

20 (3) Employ automated tools to continuously
21 monitor general purpose computers, servers, and
22 mobile devices for active, up-to-date anti-malware
23 protection with antivirus, antispysware, personal fire-
24 walls, and host-based intrusion prevention system
25 functionality.

1 (4) Centralize oversight and control to effec-
2 tively administer patch management processes (but
3 the responsibility for testing and applying patches to
4 specific systems may be decentralized to the compo-
5 nent level).

6 (5) Perform regular scans of general purpose
7 computers and servers to discover security
8 vulnerabilities and log the results of such scans.

9 (6) Perform a patch-focused risk assessment to
10 evaluate each system, database, and general purpose
11 computer for threats, vulnerabilities, and its criti-
12 cality to the mission of the Department.

13 (7) If the Secretary determines any security
14 vulnerability—

15 (A) develop a test for the vulnerability and
16 determine the cause of the vulnerability;

17 (B) address the vulnerability, including by
18 patching, implementing a compensating control,
19 or documenting and accepting a reasonable
20 business risk (in accordance with industry ac-
21 cepted best practices) with respect to the vul-
22 nerability; and

23 (C) perform a post remediation scan to
24 verify that the vulnerability was so addressed.

1 (8) Establish and ensure the use of standard,
2 secure configurations of each operating system in
3 use on the computers of the Department.

4 (9) Employ system-scanning tools that check
5 computers daily for software version, patch levels,
6 and configuration files.

7 (10) Deploy a security content automation pro-
8 tocol tool that is validated by the National Institute
9 of Standards and Technology to use specific stand-
10 ards to enable automated vulnerability management,
11 measurement, and policy compliance evaluation.

12 (11) Standardize policies, procedures, and tools
13 for effective patch management, including by assign-
14 ing roles and responsibilities, performing risk assess-
15 ments, and testing patches.

16 (12) Test each patch against all system con-
17 figurations of the Department in a test environment
18 to determine any effect on the network before de-
19 ploying the patch to the affected systems and mon-
20 itor the status of the patches after deployment.

21 (13) Establish and maintain an inventory of all
22 hardware equipment, software packages, services,
23 and other technologies installed and used by the De-
24 partment for patch management.

1 (14) Establish a policy for security fixes that is
2 clearly communicated to computer users to ensure
3 that the users are aware of—

4 (A) the versions of software or operating
5 systems that are supported with respect to se-
6 curity fixes; and

7 (B) when software, operating systems, or
8 other products are scheduled to no longer be
9 maintained.

10 (15) Ensure that—

11 (A) the staff or contractors of the Depart-
12 ment who are involved in patch management
13 have the skills and knowledge needed to per-
14 form the responsibilities relating to such man-
15 agement; and

16 (B) system administrators are trained in
17 identifying new patches and vulnerabilities.

18 (c) CERTIFICATION.—Not later than 30 days after
19 the date of the enactment of this Act, the Secretary shall
20 submit to the congressional veterans committees written
21 certification that the Secretary has commenced each ac-
22 tion described in subsection (b).

1 **SEC. 5. UPGRADE OR PHASE-OUT OF UNSUPPORTED OR**
2 **OUTDATED OPERATING SYSTEMS.**

3 (a) IN GENERAL.—Not later than 90 days after the
4 date of the enactment of this Act, the Secretary shall en-
5 sure that the Secretary upgrades or phases out outdated
6 or unsupported operating systems to protect computers of
7 the Department from harmful viruses, spyware, and other
8 malicious software that could affect the confidentiality of
9 sensitive personal information of veterans.

10 (b) ACTIONS REQUIRED.—In carrying out subsection
11 (a), the Secretary shall carry out the following activities:

12 (1) Establish a plan for phasing out outdated
13 or unsupported operating systems used by the De-
14 partment.

15 (2) Establish a policy to ensure that outdated
16 and unsupported operating systems used by the De-
17 partment do not connect to the network of the De-
18 partment by not later than 15 days after the date
19 on which such operating systems are so outdated or
20 unsupported, as determined appropriate by the Sec-
21 retary.

22 (3) Establish a configuration management proc-
23 ess to ensure that—

24 (A) a secure image that is regularly up-
25 dated is used to build all new computers used
26 by the Department; and

1 (B) any computer used by the Department
2 that becomes compromised is re-imaged using
3 such image.

4 (4) Implement applicable operating systems
5 based on security guidance identified by the Infor-
6 mation Assurance Directorate of the National Secu-
7 rity Agency.

8 (5) Appropriately configure and test required
9 software that was designed to be used on older oper-
10 ating systems to ensure the software is usable on a
11 new operating system used by the Department.

12 (6) Limit administrative privileges to very few
13 users who have both the appropriate knowledge and
14 business need to modify the configuration of the op-
15 erating system.

16 (7) Until the date on which an unsupported op-
17 erating system is replaced, if a computer uses such
18 operating system, disable web browser plug-ins, use
19 a hardware firewall, and if practicable, disconnect
20 the computer from the network and do not use the
21 computer to access the Internet.

22 (8) Deploy a software inventory tool to cover
23 each of the operating systems in use by the Depart-
24 ment to track—

1 (A) the type of such operating systems
2 being used by the Department; and

3 (B) with respect to each computer of the
4 Department—

5 (i) the type of operating system in-
6 stalled and the version number and patch
7 level of such operating system; and

8 (ii) the software being used on such
9 operating system.

10 (9) Regularly use file integrity checking tools to
11 check any changes to critical operating systems,
12 services, and configuration files.

13 (c) CERTIFICATION.—Not later than 30 days after
14 the date of the enactment of this Act, the Secretary shall
15 submit to the congressional veterans committees written
16 certification that the Secretary has commenced each ac-
17 tion described in subsection (b).

18 **SEC. 6. SECURITY OF WEB APPLICATIONS FROM VITAL**
19 **VULNERABILITIES.**

20 (a) IN GENERAL.—The Secretary shall ensure that
21 web applications used by the Department are secure from
22 vulnerabilities that could affect the confidentiality of sen-
23 sitive personal information of veterans.

24 (b) ACTIONS REQUIRED.—In carrying out subsection
25 (a), the Secretary shall carry out the following activities:

1 (1) Not later than 60 days after the date of the
2 enactment of this Act, develop a plan, including re-
3 quired actions and milestones, to fully remediate all
4 security vulnerabilities described in subsection (a)
5 that exist as of the date of the enactment of this
6 Act.

7 (2) Develop detailed guidance for remediating
8 each critical security vulnerability.

9 (3) Use best practices and lessons learned, in-
10 cluding such practices and lessons described by the
11 National Institute of Standards and Technology and
12 the Open Web Application Security Project, to ad-
13 dress the security vulnerabilities of web applications.

14 (4) Limit the permissions on the database logon
15 used by web applications to only what is needed to
16 reduce the effectiveness of any attack that exploits
17 bugs in the application.

18 (5) Provide to web application developers—

19 (A) thorough application development
20 guidance to ensure that new applications are
21 designed by taking into account security; and

22 (B) detailed guidance on testing existing
23 web applications for security vulnerabilities, in-
24 cluding buffer overflows and cross-site
25 scripting.

1 (6) Configure administrative passwords to be—

2 (A) complex and consist only of strings of
3 letters, numbers, and characters that do not
4 form a recognizable word; and

5 (B) changed every 90 days, in accordance
6 with industry best practices.

7 (7) With respect to passwords used in connec-
8 tion with web applications, store the passwords for
9 each system of the Department only in a well-hashed
10 or encrypted format.

11 (8) Implement two-factor authentication tech-
12 nology requirements throughout the Department.

13 (9) If vulnerabilities in a web application are
14 found, administer a full-source code review to deter-
15 mine if the vulnerabilities exist elsewhere within the
16 code of the application.

17 (10) Periodically review user access to networks
18 and web applications to identify unnecessary, inac-
19 tive, or terminated user accounts.

20 (11) Establish a single set of strong authentica-
21 tion and session management controls that meet all
22 the authentication and session management require-
23 ments defined in the Application Security
24 Verification Standard of the Open Web Application
25 Security Project.

1 (12) Implement visibility and attribution meas-
2 ures to improve the process, architecture, and tech-
3 nical capabilities of the Department to monitor web
4 applications used on the networks and computers of
5 the Department to detect attack attempts, locate
6 points of entry, identify already compromised ma-
7 chines, interrupt activities of infiltrated attackers,
8 and gain information about the sources of an attack.

9 (c) CERTIFICATION.—Not later than 30 days after
10 the date of the enactment of this Act, the Secretary shall
11 submit to the congressional veterans committees written
12 certification that the Secretary has commenced each ac-
13 tion described in subsection (b).

14 **SEC. 7. SECURITY OF THE VISTA SYSTEM.**

15 (a) IN GENERAL.—Not later than 90 days after the
16 date of the enactment of this Act, the Secretary shall en-
17 sure that the Vista system is secure from vulnerabilities
18 that could affect the confidentiality of sensitive personal
19 information of veterans.

20 (b) ACTIONS REQUIRED.—In carrying out subsection
21 (a), the Secretary shall carry out the following activities:

22 (1) Develop a remedial action plan to address
23 the approaches to interoperability—

24 (A) between multiple Vista systems; and

1 (B) between the Vista system and external
2 systems and software.

3 (2) Update the policy, procedures, and govern-
4 ance of the Department with respect to system-to-
5 system integration where users log on to external
6 systems and then automatically connect to the Vista
7 system and interact.

8 (3) Provide authentication for the machine-to-
9 machine broker so that the Vista system “listener”
10 verifies the identity of the calling system.

11 (4) Establish and implement policy with respect
12 to the authentication of external systems attempting
13 to connect to the Vista system and criteria by which
14 user authentication must be accomplished to ensure
15 all applications that connect to the Vista system con-
16 vey accurate user information.

17 (5) Establish a business requirement that sys-
18 tem-to-system integration connectivity across the
19 wide-area network must consist of encrypted com-
20 munication and require external systems to securely
21 identify themselves, or for the Vista system to se-
22 curely identify external systems that attempt to con-
23 nect to the system.

24 (6) Establish a business requirement that exter-
25 nal systems communicate accurate user information

1 to the Vista system relating to actions initiated by
2 actual individuals and facilitate the revocation of ac-
3 cess by the Vista system relative to specific users or
4 external systems attempting to connect.

5 (7) Implement monthly project design reviews
6 of the integration between systems and web applica-
7 tions to ensure that the effectiveness of the existing
8 controls is sustained.

9 (8) Assess the potential compromise to non-De-
10 partment networks that are interconnected with the
11 network of the Department, including the networks
12 of the Department of Defense and the Department
13 of Health and Human Services.

14 (9) Ensure that, in the near-term, software de-
15 velopment for the Vista system develops the critical
16 enhancements and fixes to the system that are nec-
17 essary to ensure compliance with changes to patient
18 enrollment.

19 (10) Ensure that all systems of the Department
20 have been given the “Authority to Operate” designa-
21 tion and have been properly certified by meeting all
22 requirements, including a comprehensive assessment
23 of management, operational, and technical security
24 controls, to become operational, and restrict the use
25 of waivers.

1 (c) CERTIFICATION.—Not later than 30 days after
2 the date of the enactment of this Act, the Secretary shall
3 submit to the congressional veterans committees written
4 certification that the Secretary has commenced each ac-
5 tion described in subsection (b).

6 **SEC. 8. REPORT ON COMPLIANCE WITH INFORMATION SE-**
7 **CURITY REQUIREMENTS AND BEST PRAC-**
8 **TICES.**

9 Not later than 60 days after the date of the enact-
10 ment of this Act, the Secretary of Veterans Affairs shall
11 submit to the congressional veterans committees the fol-
12 lowing:

13 (1) Written certification that the Secretary is
14 taking every action required to comply with—

15 (A) subchapter III of chapter 57 of title
16 38, United States Code;

17 (B) subchapter III of chapter 35 of title
18 44, United States Code;

19 (C) special publications 800–53 and 800–
20 111 of the National Institute of Standards and
21 Technology, including with respect to
22 encrypting databases;

23 (D) applicable memoranda issued by the
24 Director of Management and Budget regarding

1 protecting personally identifiable information;
2 and

3 (E) any other relevant law or regulation
4 regarding the information security of the De-
5 partment of Veterans Affairs.

6 (2) How the Secretary is using and imple-
7 menting the principles and best practices regarding
8 improving information security, including with re-
9 spect to such principles and practices described in
10 the document titled “Framework for Improving Crit-
11 ical Infrastructure Cybersecurity” of the National
12 Institute of Standards and Technology.

13 **SEC. 9. REPORTS ON IMPLEMENTATION.**

14 (a) BIENNIAL REPORTS.—

15 (1) IN GENERAL.—Not later than 180 days
16 after the date of the enactment of this Act, and
17 every 180-day period thereafter, the Secretary shall
18 submit to the congressional veterans committees a
19 report on the implementation of this Act, including
20 the amendments made by this Act.

21 (2) MATTERS INCLUDED.—Each report under
22 subsection (a) shall include the following:

23 (A) A description of the actions taken by
24 the Secretary to implement and comply with
25 sections 2 through 7.

1 (B) A timeline and project plan, both
2 short-term and long-term, for implementing
3 each of sections 2 through 7 and assigning roles
4 and responsibilities under such plan.

5 (C) Performance measures and bench-
6 marks to measure the results of the Secretary
7 in carrying out remediation efforts under sec-
8 tions 2 through 7.

9 (D) A description of the best practices and
10 lessons learned by the Secretary in carrying out
11 sections 2 through 7.

12 (E) The progress made by the Secretary
13 during each month covered by the report with
14 respect to reducing the total number of out-
15 dated operating systems, web application
16 vulnerabilities, critical security vulnerabilities,
17 and other matters covered by sections 2
18 through 7.

19 (F) An appendix containing detailed re-
20 ports of the Department, including the enter-
21 prise information technology dashboard and re-
22 ports regarding security vulnerabilities, oper-
23 ating system trends, and web applications.

24 (b) ANNUAL INSPECTOR GENERAL REPORT.—The
25 Inspector General of the Department of Veterans Affairs

1 shall submit to the congressional veterans committees an
2 annual report that includes a comprehensive assessment
3 of the adequacy and effectiveness of the implementation
4 by the Secretary of Veterans Affairs of sections 2 through
5 7, including the amendments made by this Act.

6 (c) MONTHLY REPORTS.—On a monthly basis, the
7 Secretary shall submit to the congressional veterans com-
8 mittees reports on security vulnerabilities discovered pur-
9 suant to the actions taken under section 4(b)(5).

10 **SEC. 10. APPLICATION.**

11 In carrying out this Act, including the amendments
12 made by this Act, the Secretary of Veterans Affairs may
13 substitute a new technology or process relating to informa-
14 tion security for a specific technology or process relating
15 to information security described in this Act, including the
16 amendments made by this Act, if the Secretary determines
17 that such new technology or process—

18 (1) is a successor to the specific technology or
19 process described in this Act, including the amend-
20 ments made by this Act; and

21 (2) provides a greater amount of information
22 security than would be provided if the Secretary did
23 not make such substitution.

24 **SEC. 11. DEFINITIONS.**

25 In this Act:

1 (1) The term “Authority to Operate” means the
2 official management decision given by a senior offi-
3 cial of the Department to authorize operation of an
4 information system and to explicitly accept the risk
5 to the operations of the Department (including with
6 respect to the mission, functions, image, or reputa-
7 tion of the Department), the assets and individuals
8 of the Department, other elements of the Federal
9 Government, and the United States based on the im-
10 plementation of an agreed-upon set of security con-
11 trols.

12 (2) The terms “confidentiality” has the mean-
13 ing given that term in section 5727 of title 38,
14 United States Code.

15 (3) The term “congressional veterans commit-
16 tees” means the Committees on Veterans’ Affairs of
17 the House of Representatives and the Senate.

18 (4) The term “critical network infrastructure”
19 means information technology hardware that pro-
20 vides—

21 (A) vital network services to the Depart-
22 ment that is vital to carrying out the mission
23 of the Department; and

1 (B) communications, security, transpor-
2 tation, access, and authentication services and
3 capabilities.

4 (5) The term “domain controller” means a
5 server that responds to security authentication re-
6 quests responsible for allowing host access to domain
7 resources by authenticating users, sorting user ac-
8 count information, and enforcing security policy.

9 (6) The term “general purpose computer”
10 means a computer that, given the appropriate appli-
11 cation and required time, should be able to perform
12 most common computing tasks. Such term includes
13 personal computers, including desktops, notebooks,
14 smart phones, and tablets.

15 (7) The term “image” means a standard set of
16 software (including the operating system and other
17 software) that is installed on a computer.

18 (8) The term “information security” has the
19 meaning given that term in section 5727 of title 38,
20 United States Code.

21 (9) The term “information system” has the
22 meaning given that term in section 5727 of title 38,
23 United States Code.

1 (10) The term “sensitive personal information”
2 has the meaning given that term in section 5727 of
3 title 38, United States Code.

4 (11) The term “Vista system” means the Vet-
5 erans Health Information Systems and Technology
6 Architecture of the Department of Veterans Affairs
7 that allows for an integrated inpatient and out-
8 patient electronic health record for patients and pro-
9 vides administrative tools to employees of the De-
10 partment.

11 (12) The term “web application” means an ap-
12 plication in which all or some parts of the software
13 are downloaded from the Internet each time the soft-
14 ware is accessed, including web browser-based soft-
15 ware that run within a web browser, desktop soft-
16 ware that does not use a web browser, and mobile
17 software that accesses the Internet for additional in-
18 formation.

19 (13) The term “well-hashed” means the process
20 of using a mathematical algorithm against data to
21 produce a numeric value that is representative of
22 that data.