

113TH CONGRESS  
2D SESSION

# H. R. 4370

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

APRIL 2, 2014

Mrs. WALORSKI (for herself, Mr. COFFMAN, Mr. WENSTRUP, and Mr. NUGENT) introduced the following bill; which was referred to the Committee on Veterans' Affairs

---

## 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”.

6 (b) TABLE OF CONTENTS.—The table of contents for  
7 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.

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

4 (a) REQUIREMENTS FOR CERTAIN OFFICIALS AND  
 5 STAFF.—

6 (1) IN GENERAL.—Subchapter III of chapter  
 7 57 of title 38, United States Code, is amended by  
 8 inserting after section 5723 the following new sec-  
 9 tion:

10 **“§ 5723A. Governance of information security pro-**  
 11 **gram**

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

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

17 (1) The Secretary shall ensure that the Assistant Sec-  
 18 retary for Information and Technology, as the Chief Infor-  
 19 mation Officer of the Department, possesses—

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

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

7           “(C) demonstrated, sound technical capabilities.

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

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

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

22               “(B) validate that each third-party developed  
23               software used in any information system of the De-  
24               partment meets the standards of the National Insti-  
25               tute of Standards and Technology with respect to

1 security, safety, reliability, functionality and extensi-  
2 bility;

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

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

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

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

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

23 “(B) an industry recognized certification in  
24 cyber security defense;

1           “(C) demonstrated, sound technical capabilities;  
2           and  
3           “(D) other relevant experience.

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

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

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

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

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

23           “(25) DATA WAREHOUSE.—The term ‘data  
24 warehouse’ means a collection of data designed to  
25 support management decision making that contains

1 a wide variety of data that present a coherent pic-  
2 ture of business conditions for an entire organization  
3 at a single point in time and whose development in-  
4 cludes the development of systems to extract data  
5 from operating systems plus installation of a ware-  
6 house database system that provides managers flexi-  
7 ble access to the data.”.

8 **SEC. 3. SECURITY OF CRITICAL NETWORK INFRASTRUC-**  
9 **TURE, INCLUDING DOMAIN CONTROLLER, OF**  
10 **DEPARTMENT OF VETERANS AFFAIRS.**

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

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

18 (1) Maintain the awareness and complete phys-  
19 ical and logical control of the critical network infra-  
20 structure, including routers, switches, domain nam-  
21 ing systems, firewalls, load balancers, proxy devices,  
22 authentication services, telecommunications, domain  
23 controllers, and any device that is part of the trust-  
24 ed Internet connection system.

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

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

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

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

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

24           (7) Establish access rights, permissions, and  
25 multifactor authentication for the critical infrastruc-

1       ture devices and services, including the domain con-  
2       troller, for specific users or groups of users.

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

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

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

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

22          (12) Conduct regular audits and testing of the  
23      backups and restore events of the critical infrastruc-  
24      ture devices and services.





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

3 (1) Formalize and enforce a Department-wide  
4 process to monitor software installed on general pur-  
5 pose computers and servers of the Department, pre-  
6 vent the unauthorized installation of software, and  
7 remove any unauthorized software that has been in-  
8 stalled.

9 (2) Not later than 45 days after the date of the  
10 enactment of this Act, implement automated patch-  
11 ing tools and processes that ensure that security  
12 patches are installed for any software or operating  
13 system on a computer by not later than 48 hours  
14 after the patch is made available.

15 (3) Employ automated tools to continuously  
16 monitor general purpose computers, servers, and  
17 mobile devices for active, up-to-date anti-malware  
18 protection with antivirus, antispyware, personal fire-  
19 walls, and host-based intrusion prevention system  
20 functionality.

21 (4) Centralize oversight and control to effec-  
22 tively administer patch management processes (but  
23 the responsibility for testing and applying patches to  
24 specific systems may be decentralized to the compo-  
25 nent level).

1           (5) Perform regular scans of general purpose  
2 computers and servers to discover security vulnera-  
3 bilities and log the results of such scans.

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

8           (7) If the Secretary determines any security  
9 vulnerability—

10                   (A) develop a test for the vulnerability and  
11 determine the cause of the vulnerability;

12                   (B) address the vulnerability, including by  
13 patching, implementing a compensating control,  
14 or documenting and accepting a reasonable  
15 business risk (in accordance with industry ac-  
16 cepted best practices) with respect to the vul-  
17 nerability; and

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

20           (8) Establish and ensure the use of standard,  
21 secure configurations of each operating system in  
22 use on the computers of the Department.

23           (9) Employ system-scanning tools that check  
24 computers daily for software version, patch levels,  
25 and configuration files.

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

6           (11) Standardize policies, procedures, and tools  
7           for effective patch management, including by assign-  
8           ing roles and responsibilities, performing risk assess-  
9           ments, and testing patches.

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

15          (13) Establish and maintain an inventory of all  
16          hardware equipment, software packages, services,  
17          and other technologies installed and used by the De-  
18          partment for patch management.

19          (14) Establish a policy for security fixes that is  
20          clearly communicated to computer users to ensure  
21          that the users are aware of—

22                 (A) the versions of software or operating  
23                 systems that are supported with respect to se-  
24                 curity fixes; and

1           (B) when software, operating systems, or  
2 other products are scheduled to no longer be  
3 maintained.

4           (15) Ensure that—

5           (A) the staff or contractors of the Depart-  
6 ment who are involved in patch management  
7 have the skills and knowledge needed to per-  
8 form the responsibilities relating to such man-  
9 agement; and

10           (B) system administrators are trained in  
11 identifying new patches and vulnerabilities.

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

17 **SEC. 5. UPGRADE OR PHASE-OUT OF UNSUPPORTED OR**  
18 **OUTDATED OPERATING SYSTEMS.**

19           (a) IN GENERAL.—Not later than 90 days after the  
20 date of the enactment of this Act, the Secretary shall en-  
21 sure that the Secretary upgrades or phases out outdated  
22 or unsupported operating systems to protect computers of  
23 the Department from harmful viruses, spyware, and other  
24 malicious software that could affect the confidentiality of  
25 sensitive personal information of veterans.

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

3 (1) Establish a plan for phasing out outdated  
4 or unsupported operating systems used by the De-  
5 partment.

6 (2) Establish a policy to ensure that outdated  
7 and unsupported operating systems used by the De-  
8 partment do not connect to the network of the De-  
9 partment by not later than 15 days after the date  
10 on which such operating systems are so outdated or  
11 unsupported, as determined appropriate by the Sec-  
12 retary.

13 (3) Establish a configuration management proc-  
14 ess to ensure that—

15 (A) a secure image that is regularly up-  
16 dated is used to build all new computers used  
17 by the Department; and

18 (B) any computer used by the Department  
19 that becomes compromised is re-imaged using  
20 such image.

21 (4) Implement applicable operating systems  
22 based on security guidance identified by the Infor-  
23 mation Assurance Directorate of the National Secu-  
24 rity Agency.

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

5           (6) Limit administrative privileges to very few  
6 users who have both the appropriate knowledge and  
7 business need to modify the configuration of the op-  
8 erating system.

9           (7) Until the date on which an unsupported op-  
10 erating system is replaced, if a computer uses such  
11 operating system, disable web browser plug-ins, use  
12 a hardware firewall, and if practicable, disconnect  
13 the computer from the network and do not use the  
14 computer to access the Internet.

15           (8) Deploy a software inventory tool to cover  
16 each of the operating systems in use by the Depart-  
17 ment to track—

18                   (A) the type of such operating systems  
19 being used by the Department; and

20                   (B) with respect to each computer of the  
21 Department—

22                           (i) the type of operating system in-  
23 stalled and the version number and patch  
24 level of such operating system; and

1 (ii) the software being used on such  
2 operating system.

3 (9) Regularly use file integrity checking tools to  
4 check any changes to critical operating systems,  
5 services, and configuration files.

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

11 **SEC. 6. SECURITY OF WEB APPLICATIONS FROM VITAL**  
12 **VULNERABILITIES.**

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

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

19 (1) Not later than 60 days after the date of the  
20 enactment of this Act, develop a plan, including re-  
21 quired actions and milestones, to fully remediate all  
22 security vulnerabilities described in subsection (a)  
23 that exist as of the date of the enactment of this  
24 Act.



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

3           (3) Use best practices and lessons learned, in-  
4 cluding such practices and lessons described by the  
5 National Institute of Standards and Technology and  
6 the Open Web Application Security Project, to ad-  
7 dress the security vulnerabilities of web applications.

8           (4) Limit the permissions on the database logon  
9 used by web applications to only what is needed to  
10 reduce the effectiveness of any attack that exploits  
11 bugs in the application.

12           (5) Provide to web application developers—

13                 (A) thorough application development  
14 guidance to ensure that new applications are  
15 designed by taking into account security; and

16                 (B) detailed guidance on testing existing  
17 web applications for security vulnerabilities, in-  
18 cluding buffer overflows and cross-site script-  
19 ing.

20           (6) Configure administrative passwords to be—

21                 (A) complex and consist only of strings of  
22 letters, numbers, and characters that do not  
23 form a recognizable word; and

24                 (B) changed every 90 days, in accordance  
25 with industry best practices.

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

5           (8) Implement two-factor authentication tech-  
6           nology requirements throughout the Department.

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

11          (10) Periodically review user access to networks  
12          and web applications to identify unnecessary, inac-  
13          tive, or terminated user accounts.

14          (11) Establish a single set of strong authentica-  
15          tion and session management controls that meet all  
16          the authentication and session management require-  
17          ments defined in the Application Security Verifica-  
18          tion Standard of the Open Web Application Security  
19          Project.

20          (12) Implement visibility and attribution meas-  
21          ures to improve the process, architecture, and tech-  
22          nical capabilities of the Department to monitor web  
23          applications used on the networks and computers of  
24          the Department to detect attack attempts, locate  
25          points of entry, identify already compromised ma-

1 chines, interrupt activities of infiltrated attackers,  
2 and gain information about the sources of an attack.

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

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

9 (a) IN GENERAL.—Not later than 90 days after the  
10 date of the enactment of this Act, the Secretary shall en-  
11 sure that the Vista system is secure from vulnerabilities  
12 that could affect the confidentiality of sensitive personal  
13 information of veterans.

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

16 (1) Develop a remedial action plan to address  
17 the approaches to interoperability—

18 (A) between multiple Vista systems; and

19 (B) between the Vista system and external  
20 systems and software.

21 (2) Update the policy, procedures, and govern-  
22 ance of the Department with respect to system-to-  
23 system integration where users log on to external  
24 systems and then automatically connect to the Vista  
25 system and interact.

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

4           (4) Establish and implement policy with respect  
5 to the authentication of external systems attempting  
6 to connect to the Vista system and criteria by which  
7 user authentication must be accomplished to ensure  
8 all applications that connect to the Vista system con-  
9 vey accurate user information.

10          (5) Establish a business requirement that sys-  
11 tem-to-system integration connectivity across the  
12 wide-area network must consist of encrypted com-  
13 munication and require external systems to securely  
14 identify themselves, or for the Vista system to se-  
15 curely identify external systems that attempt to con-  
16 nect to the system.

17          (6) Establish a business requirement that exter-  
18 nal systems communicate accurate user information  
19 to the Vista system relating to actions initiated by  
20 actual individuals and facilitate the revocation of ac-  
21 cess by the Vista system relative to specific users or  
22 external systems attempting to connect.

23          (7) Implement monthly project design reviews  
24 of the integration between systems and web applica-

1 tions to ensure that the effectiveness of the existing  
2 controls is sustained.

3 (8) Assess the potential compromise to non-De-  
4 partment networks that are interconnected with the  
5 network of the Department, including the networks  
6 of the Department of Defense and the Department  
7 of Health and Human Services.

8 (9) Ensure that, in the near-term, software de-  
9 velopment for the Vista system develops the critical  
10 enhancements and fixes to the system that are nec-  
11 essary to ensure compliance with changes to patient  
12 enrollment.

13 (10) Ensure that all systems of the Department  
14 have been given the “Authority to Operate” designa-  
15 tion and have been properly certified by meeting all  
16 requirements, including a comprehensive assessment  
17 of management, operational, and technical security  
18 controls, to become operational, and restrict the use  
19 of waivers.

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

1 **SEC. 8. REPORT ON COMPLIANCE WITH INFORMATION SE-**  
2 **CURITY REQUIREMENTS AND BEST PRAC-**  
3 **TICES.**

4 Not later than 60 days after the date of the enact-  
5 ment of this Act, the Secretary of Veterans Affairs shall  
6 submit to the congressional veterans committees the fol-  
7 lowing:

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

10 (A) subchapter III of chapter 57 of title  
11 38, United States Code;

12 (B) subchapter III of chapter 35 of title  
13 44, United States Code;

14 (C) special publications 800–53 and 800–  
15 111 of the National Institute of Standards and  
16 Technology, including with respect to encrypt-  
17 ing databases;

18 (D) applicable memoranda issued by the  
19 Director of Management and Budget regarding  
20 protecting personally identifiable information;  
21 and

22 (E) any other relevant law or regulation  
23 regarding the information security of the De-  
24 partment of Veterans Affairs.

25 (2) How the Secretary is using and imple-  
26 menting the principles and best practices regarding

1 improving information security, including with re-  
2 spect to such principles and practices described in  
3 the document titled “Framework for Improving Crit-  
4 ical Infrastructure Cybersecurity” of the National  
5 Institute of Standards and Technology.

6 **SEC. 9. REPORTS ON IMPLEMENTATION.**

7 (a) BIENNIAL REPORTS.—

8 (1) IN GENERAL.—Not later than 180 days  
9 after the date of the enactment of this Act, and  
10 every 180-day period thereafter, the Secretary shall  
11 submit to the congressional veterans committees a  
12 report on the implementation of this Act, including  
13 the amendments made by this Act.

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

16 (A) A description of the actions taken by  
17 the Secretary to implement and comply with  
18 sections 2 through 7.

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

23 (C) Performance measures and bench-  
24 marks to measure the results of the Secretary

1 in carrying out remediation efforts under sec-  
2 tions 2 through 7.

3 (D) A description of the best practices and  
4 lessons learned by the Secretary in carrying out  
5 sections 2 through 7.

6 (E) The progress made by the Secretary  
7 during each month covered by the report with  
8 respect to reducing the total number of out-  
9 dated operating systems, web application vul-  
10 nerabilities, critical security vulnerabilities, and  
11 other matters covered by sections 2 through 7.

12 (F) An appendix containing detailed re-  
13 ports of the Department, including the enter-  
14 prise information technology dashboard and re-  
15 ports regarding security vulnerabilities, oper-  
16 ating system trends, and web applications.

17 (b) ANNUAL INSPECTOR GENERAL REPORT.—The  
18 Inspector General of the Department of Veterans Affairs  
19 shall submit to the congressional veterans committees an  
20 annual report that includes a comprehensive assessment  
21 of the adequacy and effectiveness of the implementation  
22 by the Secretary of Veterans Affairs of sections 2 through  
23 7, including the amendments made by this Act.

24 (c) MONTHLY REPORTS.—On a monthly basis, the  
25 Secretary shall submit to the congressional veterans com-



1 mitted reports on security vulnerabilities discovered pur-  
2 suant to the actions taken under section 4(b)(5).

3 **SEC. 10. APPLICATION.**

4 In carrying out this Act, including the amendments  
5 made by this Act, the Secretary of Veterans Affairs may  
6 substitute a new technology or process relating to informa-  
7 tion security for a specific technology or process relating  
8 to information security described in this Act, including the  
9 amendments made by this Act, if the Secretary determines  
10 that such new technology or process—

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

14 (2) provides a greater amount of information  
15 security than would be provided if the Secretary did  
16 not make such substitution.

17 **SEC. 11. DEFINITIONS.**

18 In this Act:

19 (1) The term “Authority to Operate” means the  
20 official management decision given by a senior offi-  
21 cial of the Department to authorize operation of an  
22 information system and to explicitly accept the risk  
23 to the operations of the Department (including with  
24 respect to the mission, functions, image, or reputa-  
25 tion of the Department), the assets and individuals

1 of the Department, other elements of the Federal  
2 Government, and the United States based on the im-  
3 plementation of an agreed-upon set of security con-  
4 trols.

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

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

11 (4) The term “critical network infrastructure”  
12 means information technology hardware that pro-  
13 vides—

14 (A) vital network services to the Depart-  
15 ment that is vital to carrying out the mission  
16 of the Department; and

17 (B) communications, security, transpor-  
18 tation, access, and authentication services and  
19 capabilities.

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

1           (6) The term “general purpose computer”  
2 means a computer that, given the appropriate appli-  
3 cation and required time, should be able to perform  
4 most common computing tasks. Such term includes  
5 personal computers, including desktops, notebooks,  
6 smart phones, and tablets.

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

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

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

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

19          (11) The term “Vista system” means the Vet-  
20 erans Health Information Systems and Technology  
21 Architecture of the Department of Veterans Affairs  
22 that allows for an integrated inpatient and out-  
23 patient electronic health record for patients and pro-  
24 vides administrative tools to employees of the De-  
25 partment.

1           (12) The term “web application” means an ap-  
2           plication in which all or some parts of the software  
3           are downloaded from the Internet each time the soft-  
4           ware is accessed, including web browser-based soft-  
5           ware that run within a web browser, desktop soft-  
6           ware that does not use a web browser, and mobile  
7           software that accesses the Internet for additional in-  
8           formation.

9           (13) The term “well-hashed” means the process  
10          of using a mathematical algorithm against data to  
11          produce a numeric value that is representative of  
12          that data.

○