''Photographs or microphotographs of records'' and substituted ''photographs, microphotographs, or digitized records'' for ''photographs or microphotographs'' in two places.

§ 3313. Moneys from sale of records payable into the Treasury

Moneys derived by agencies of the Government from the sale of records disposed of under this chapter shall be paid into the Treasury of the United States unless otherwise required by law.

(Pub. L. 90–620, Oct. 22, 1968, 82 Stat. 1302.)

HISTORICAL AND REVISION NOTES

Based on 44 U.S. Code, 1964 ed., § 379 (July 7, 1943, ch. 192, § 14, 57 Stat. 383).

§ 3314. Procedures for disposal of records exclusive

The procedures prescribed by this chapter are exclusive, and records of the United States Government may not be alienated or destroyed except under this chapter.

(Pub. L. 90–620, Oct. 22, 1968, 82 Stat. 1302.)

HISTORICAL AND REVISION NOTES

Based on 44 U.S. Code, 1964 ed., § 380 (July 7, 1943, ch. 192, § 15, 57 Stat. 383).

[§§ 3315 to 3324. Repealed. Pub. L. 113–187, § 7(a), Nov. 26, 2014, 128 Stat. 2011]

Section 3315, added Pub. L. 93–526, title II, § 202, Dec. 19, 1974, 88 Stat. 1698, related to definitions of certain terms used in sections 3315 to 3324.

Section 3316, added Pub. L. 93–526, title II, § 202, Dec. 19, 1974, 88 Stat. 1699, related to the establishment of the National Study Commission on Records and Documents of Federal Officials.

Section 3317, added Pub. L. 93–526, title II, § 202, Dec. 19, 1974, 88 Stat. 1699, related to the duties of the Commission.

Section 3318, added Pub. L. 93–526, title II, § 202, Dec. 19, 1974, 88 Stat. 1699; amended Pub. L. 94–261, § 1(a), Apr. 11, 1976, 90 Stat. 326, related to membership of the Commission.

Section 3319, added Pub. L. 93–526, title II, § 202, Dec. 19, 1974, 88 Stat. 1701, related to director, staff, experts, and consultants.

Section 3320, added Pub. L. 93–526, title II, § 202, Dec. 19, 1974, 88 Stat. 1701, related to the powers of the Commission.

Section 3321, added Pub. L. 93–526, title II, § 202, Dec. 19, 1974, 88 Stat. 1701, related to support services provided to the Commission by the Administrator of General Services and the Archivist of the United States.

Section 3322, added Pub. L. 93–526, title II, § 202, Dec. 19, 1974, 88 Stat. 1701; amended Pub. L. 94–261, § 1(b), Apr. 11, 1976, 90 Stat. 326, related to the report of the Commission.

Section 3323, added Pub. L. 93–526, title II, § 202, Dec. 19, 1974, 88 Stat. 1701, related to termination of the Commission.

Section 3324, added Pub. L. 93–526, title II, § 202, Dec. 19, 1974, 88 Stat. 1701, related to authorization of appropriations.

CHAPTER 35—COORDINATION OF FEDERAL INFORMATION POLICY

SUBCHAPTER I—FEDERAL INFORMATION POLICY

Editorial Notes

CODIFICATION

This chapter was originally added by Pub. L. 90–620, Oct. 22, 1968, 82 Stat. 1302, which act enacted this title, and was based on act Dec. 24, 1942, ch. 811, 56 Stat. 1078, known as the Federal Reports Act of 1942, which was

classified to sections 139 to 139f of former Title 5, transferred to chapter 12 (§ 421 et seq.) of former Title 44, and repealed by Pub. L. 90–620 upon the enactment of this title. Subsequent to its original enactment by Pub. L. 90–620, this chapter was amended generally by Pub. L. 96–511 and again by Pub. L. 104–13. As a result, this chapter is shown herein as having been added beginning with Pub. L. 104–13 without reference to earlier amendatory laws. See Prior Provisions notes throughout this chapter.

AMENDMENTS

2019—Pub. L. 115–435, title II, § 202(d)(2)(A), (e)(2), (f)(2), title III, §§ 302(b), 303(b), Jan. 14, 2019, 132 Stat. 5541–5543, 5552, 5556, substituted ''Data inventory and Federal data catalogue'' for ''Establishment and operation of Government Information Locator Service'' in item 3511 and ''Chief Data Officers'' for ''Establishment of task force on information collection and dissemination'' in item 3520, added item 3520A, and added heading for subchapter III, headings for parts A to D of subchapter III, and items 3561 to 3564, 3571, 3572, 3575, 3576, and 3581 to 3583.

2018—Pub. L. 115–114, § 2(b), Jan. 10, 2018, 131 Stat. 2278, added item 3559.

2014—Pub. L. 113–283, § 2(e)(1), Dec. 18, 2014, 128 Stat. 3086, added heading for subchapter II and items 3551 to 3558 and struck out heading for former subchapter II and items 3531 to 3538 and heading for subchapter III and items 3541 to 3549. Prior to amendment, headings for both subchapters II and III read ''INFORMATION SECURITY'' and items under each subchapter were substantially similar to items 3551 to 3558.

2002—Pub. L. 107–347, title III, § 301(b)(2), Dec. 17, 2002, 116 Stat. 2955, added heading for subchapter III and items 3541 to 3549.

Pub. L. 107–296, title X, § 1001(b)(2), Nov. 25, 2002, 116 Stat. 2267, reenacted items 3531 to 3535 without change, substituted ''National security systems'' for ''Expiration'' in item 3536, and added items 3537 and 3538.

Pub. L. 107–198, § 3(b), June 28, 2002, 116 Stat. 732, added item 3520 and renumbered former item 3520 as 3521.

2000—Pub. L. 106–398, § 1 [[div. A], title X, § 1064(a)(1)], Oct. 30, 2000, 114 Stat. 1654, 1654A–275, inserted subchapters I and II headings and added items 3531 to 3536.

1995—Pub. L. 104–13, § 2, May 22, 1995, 109 Stat. 163, amended chapter heading and analysis generally.

1980—Pub. L. 96–511, § 2(a), Dec. 11, 1980, 94 Stat. 2812, substituted in chapter heading ''INFORMATION POLICY'' for ''REPORTING SERVICES'', and amended analysis generally.

SUBCHAPTER I—FEDERAL INFORMATION POLICY

Editorial Notes

AMENDMENTS

2000—Pub. L. 106–398, § 1 [[div. A], title X, § 1064(a)(2)], Oct. 30, 2000, 114 Stat. 1654, 1654A–275, inserted subchapter heading.

§ 3501. Purposes

The purposes of this subchapter are to—

(1) minimize the paperwork burden for individuals, small businesses, educational and nonprofit institutions, Federal contractors, State, local and tribal governments, and other persons resulting from the collection of information by or for the Federal Government;

(2) ensure the greatest possible public benefit from and maximize the utility of information created, collected, maintained, used, shared and disseminated by or for the Federal Government;

(3) coordinate, integrate, and to the extent practicable and appropriate, make uniform Federal information resources management policies and practices as a means to improve the productivity, efficiency, and effectiveness of Government programs, including the reduction of information collection burdens on the public and the improvement of service delivery to the public;

(4) improve the quality and use of Federal information to strengthen decisionmaking, accountability, and openness in Government and society;

(5) minimize the cost to the Federal Government of the creation, collection, maintenance, use, dissemination, and disposition of information;

(6) strengthen the partnership between the Federal Government and State, local, and tribal governments by minimizing the burden and maximizing the utility of information created, collected, maintained, used, disseminated, and retained by or for the Federal Government;

(7) provide for the dissemination of public information on a timely basis, on equitable terms, and in a manner that promotes the utility of the information to the public and makes effective use of information technology;

(8) ensure that the creation, collection, maintenance, use, dissemination, and disposition of information by or for the Federal Government is consistent with applicable laws, including laws relating to—

(A) privacy and confidentiality, including section 552a of title 5;

(B) security of information, including section 11332 of title 40[1]; and

(C) access to information, including section 552 of title 5;

(9) ensure the integrity, quality, and utility of the Federal statistical system;

(10) ensure that information technology is acquired, used, and managed to improve performance of agency missions, including the reduction of information collection burdens on the public; and

(11) improve the responsibility and accountability of the Office of Management and Budget and all other Federal agencies to Congress and to the public for implementing the information collection review process, information resources management, and related policies and guidelines established under this subchapter.

(Added Pub. L. 104–13, § 2, May 22, 1995, 109 Stat. 163; amended Pub. L. 106–398, § 1 [[div. A], title X, § 1064(b)], Oct. 30, 2000, 114 Stat. 1654, 1654A–275; Pub. L. 107–217, § 3(*l*)(3), Aug. 21, 2002, 116 Stat. 1301.)

Editorial Notes

REFERENCES IN TEXT

Section 11332 of title 40, referred to in par. (8)(B), was repealed by Pub. L. 107–296, title X, § 1005(a)(1), Nov. 25, 2002, 116 Stat. 2272, and Pub. L. 107–347, title III, § 305(a), Dec. 17, 2002, 116 Stat. 2960.

PRIOR PROVISIONS

A prior section 3501, added Pub. L. 96–511, § 2(a), Dec. 11, 1980, 94 Stat. 2812; amended Pub. L. 99–500, § 101(m)

[1] See References in Text note below.

[title VIII, § 811], Oct. 18, 1986, 100 Stat. 1783–308, 1783–335, and Pub. L. 99–591, § 101(m) [title VIII, § 811], Oct. 30, 1986, 100 Stat. 3341–308, 3341–335, related to purposes of this chapter prior to the general amendment of this chapter by Pub. L. 104–13.

Another prior section 3501, Pub. L. 90–620, Oct. 22, 1968, 82 Stat. 1302, related to information for Federal agencies, prior to the general amendment of this chapter by Pub. L. 96–511.

AMENDMENTS

2002—Par. (8)(B). Pub. L. 107–217 substituted ''section 11332 of title 40'' for ''the Computer Security Act of 1987 (Public Law 100–235)''.

2000—Pub. L. 106–398 substituted ''subchapter'' for ''chapter'' in introductory provisions and in par. (11).

Statutory Notes and Related Subsidiaries

EFFECTIVE DATE OF 2000 AMENDMENT

Amendment by Pub. L. 106–398 effective 30 days after Oct. 30, 2000, see section 1 [[div. A], title X, § 1065] of Pub. L. 106–398, Oct. 30, 2000, 114 Stat. 1654, formerly set out as an Effective Date note under former section 3531 of this title.

EFFECTIVE DATE

Pub. L. 104–13, § 4, May 22, 1995, 109 Stat. 185, provided that:

''(a) IN GENERAL.—Except as otherwise provided in this section, this Act [enacting this chapter, amending section 91 of Title 13, Census, and enacting provisions set out as a note under section 101 of this title] and the amendments made by this Act shall take effect on October 1, 1995.

''(b) AUTHORIZATION OF APPROPRIATIONS.—Section 3520 [now 3521] of title 44, United States Code, as amended by this Act, shall take effect on the date of enactment of this Act [May 22, 1995].

''(c) DELAYED APPLICATION.—In the case of a collection of information for which there is in effect on September 30, 1995, a control number issued by the Office of Management and Budget under chapter 35 of title 44, United States Code—

''(1) the amendments made by this Act [enacting this chapter and amending section 91 of Title 13] shall apply to the collection of information beginning on the earlier of—

''(A) the first renewal or modification of that collection of information after September 30, 1995; or

''(B) the expiration of its control number after September 30, 1995.

''(2) prior to such renewal, modification, or expiration, the collection of information shall be subject to chapter 35 of title 44, United States Code, as in effect on September 30, 1995.''

SHORT TITLE

This chapter is popularly known as the ''Paperwork Reduction Act''.

SOURCE CODE HARMONIZATION AND REUSE IN INFORMATION TECHNOLOGY

Pub. L. 118–187, Dec. 23, 2024, 138 Stat. 2638, provided that:

''SECTION 1. SHORT TITLE.

''This Act may be cited as the 'Source code Harmonization And Reuse in Information Technology Act' or the 'SHARE IT Act'.

''SEC. 2. DEFINITIONS.

''In this Act:

''(1) AGENCY.—The term 'agency' has the meaning given that term in section 3502 of title 44, United States Code.

''(2) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term 'appropriate congressional committees' means the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Oversight and Accountability of the House of Representatives.

''(3) CUSTOM-DEVELOPED CODE.—The term 'custom-developed code'—

''(A) means source code that is—

''(i) produced in the performance of a contract with an agency or is otherwise exclusively funded by the Federal Government; or

''(ii) developed by a Federal employee as part of the official duties of the employee;

''(B) includes—

''(i) source code, or segregable portions of source code, for which the Federal Government could obtain unlimited rights under part 27 of the Federal Acquisition Regulation or any relevant supplemental acquisition regulations of an agency; and

''(ii) source code written for a software project, module, plugin, script, middleware, or application programming interface; and

''(C) does not include—

''(i) source code that is solely exploratory or disposable in nature, including source code written by a developer experimenting with a new language or library; or

''(ii) commercial computer software, commercial off-the-shelf software, or configuration scripts for such software.

''(4) FEDERAL EMPLOYEE.—The term 'Federal employee' has the meaning given the term in section 2105(a) of title 5, United States Code.

''(5) METADATA.—The term 'metadata', with respect to custom-developed code—

''(A) has the meaning given that term in section 3502 of title 44, United States Code; and

''(B) includes—

''(i) information on whether the custom-developed code was—

''(I) produced pursuant to a contract; or

''(II) shared in a public or private repository;

''(ii) any contract number under which the custom-developed code was produced; and

''(iii) any hyperlink to the repository in such [sic] the code was shared.

''(6) PRIVATE REPOSITORY.—The term 'private repository' means a software storage location—

''(A) that contains source code, documentation, configuration scripts, as appropriate, revision history, and other files; and

''(B) access to which is restricted to only authorized users.

''(7) PUBLIC REPOSITORY.—The term 'public repository' means a software storage location—

''(A) that contains source code, documentation, configuration scripts, as appropriate, revision history, and other files; and

''(B) access to which is open to the public.

''(8) SOFTWARE.—The term 'software' has the meaning given the term 'computer software' in section 2.101 of title 48, Code of Federal Regulations, or any successor regulation.

''(9) SOURCE CODE.—The term 'source code' means a collection of computer commands written in a computer programming language that a computer can execute as a piece of software.

''SEC. 3. SOFTWARE REUSE.

''(a) SHARING.—Not later than 210 days after the date of enactment of this Act [Dec. 23, 2024], the head of each agency shall ensure that the custom-developed code of the agency and other key technical components of the code (including documentation, data models, schemas, metadata, architecture designs, configuration scripts, and artifacts required to develop, build, test, and deploy the code) of the code [sic] are—

''(1) stored at not less than 1 public repository or private repository;

''(2) accessible to Federal employees via procedures developed under subsection (d)(1)(A)(ii)(III); and

''(3) owned by the agency.

''(b) SOFTWARE REUSE RIGHTS IN PROCUREMENT CONTRACTS.—The head of an agency that enters into a contract for the custom development of software shall acquire and exercise rights sufficient to enable the governmentwide access to, sharing of, use of, and modification of any custom-developed code created in the development of such software.

''(c) DISCOVERY.—Not later than 210 days after the date of enactment of this Act, the head of each agency shall make metadata created on or after such date for the custom-developed code of the agency publicly accessible.

''(d) ACCOUNTABILITY MECHANISMS.—

''(1) AGENCY CIOS.—Not later than 180 days after the date of enactment of this Act, the Chief Information Officer of each agency, in consultation with the Chief Acquisition Officer, or similar official, of the agency and the Administrator of the Office of Electronic Government, shall develop an agency-wide policy that—

''(A) implements the requirements of this Act, including—

''(i) ensuring that custom-developed code follows the best practices established by the Director of the Office and Management and Budget under paragraph (3) for operating repositories and version control systems to keep track of changes and to facilitate collaboration among multiple developers; and

''(ii) managing the sharing of custom-developed code under subsection (b), and the public accessibility of metadata under subsection (c), including developing—

''(I) procedures to determine whether any custom-developed code meets the conditions under section 4(b) for an exemption under this Act;

''(II) procedures for making metadata for custom-developed code publicly accessible pursuant to subsection (c);

''(III) procedures for Federal employees to gain access to public repositories and private repositories that contain custom developed source code; and

''(IV) standardized reporting practices across the agency to capture key information relating to a contract under which custom-developed source code was produced for reporting statistics about the contract; and

''(B) corrects or amends any policies of the agency that are inconsistent with the requirements of this Act.

''(2) ADMINISTRATOR OF THE OFFICE OF ELECTRONIC GOVERNMENT.—

''(A) MINIMUM STANDARD REPORTING REQUIREMENTS.—Not later than 120 days after the date of enactment of this Act, the Administrator of the Office of Electronic Government shall establish minimum standard reporting requirements for the Chief Information Officers of agencies, which shall include information relating to—

''(i) measuring the frequency of reuse of code, including access and modification under subsection (b);

''(ii) whether the shared code is maintained;

''(iii) whether there is a feedback mechanism for improvements to or community development of the shared code; and

''(iv) the number and circumstances of all exemptions granted under section 4(a)(2).

''(B) REPORTING REQUIREMENT.—

''(i) REQUIREMENT.—Not later than 1 year after the date of the enactment of this Act, and annually thereafter, the Administrator of the Office of Electronic Government shall publish on a centralized website a report on the implementation of this Act that includes—

''(I) a complete list of all exemptions granted under section 4(a)(2); and

''(II) information showing whether each agency has updated the acquisition and other policies of the agency to be compliant with this Act.

''(ii) OPEN GOVERNMENT DATA ASSET.—The report under clause (i) shall be maintained as an open Government data asset (as defined in section 3502 of title 44, United States Code).

''(3) GUIDANCE.—The Director of the Office of Management and Budget shall issue guidance, consistent with the purpose of this Act, that establishes best practices and uniform procedures across agencies for the purposes of implementing this subsection.

''SEC. 4. EXEMPTIONS.

''(a) IN GENERAL.—

''(1) AUTOMATIC.—

''(A) IN GENERAL.—This Act shall not apply to classified source code or source code developed primarily for use in a national security system (as defined in section 11103 of title 40, United States Code).

''(B) NATIONAL SECURITY.—An exemption from the requirements under section 3 shall apply to classified source code or source code developed—

''(i) primarily for use in a national security system (as defined in section 11103 of title 40, United States Code); or

''(ii) by an agency, or part of an agency, that is an element of the intelligence community (as defined in section 3(4) of the National Security Act of 1947 (50 U.S.C. 3003(4))[)].

''(C) FREEDOM OF INFORMATION ACT.—An exemption from the requirements under section 3 shall apply to source code the disclosure of which is exempt under section 552(b) of title 5, United States Code (commonly known as the 'Freedom of Information Act').

''(2) DISCRETIONARY.—

''(A) EXEMPTION AND GUIDANCE.—

''(i) IN GENERAL.—The Chief Information Officer of an agency, in consultation with the Federal Privacy Council, or any successor thereto, may exempt from the requirements of section 3 any source code for which a limited exemption described in subparagraph (B) applies.

''(ii) GUIDANCE REQUIRED.—The Federal Privacy Council shall provide guidance to the Chief Information Officer of each agency relating to the limited exemption described in subparagraph (B)(ii) to ensure consistent application of this paragraph across agencies.

''(B) LIMITED EXEMPTIONS.—The limited exemptions described in this paragraph are the following:

''(i) The head of the agency is prohibited from providing the source code to another individual or entity under another Federal law or regulation, including under—

''(I) the Export Administration Regulations;

''(II) the International Traffic in Arms Regulations;

''(III) the regulations of the Transportation Security Administration relating to the protection of Sensitive Security Information; and

''(IV) the Federal laws and regulations governing the sharing of classified information not covered by the exemption in paragraph (1).

''(ii) The sharing or public accessibility of the source code would create an identifiable risk to the privacy of an individual.

''(b) REPORTS REQUIRED.—

''(1) AGENCY REPORTING.—Not later than December 31 of each year, the Chief Information Officer of an agency shall submit to the Administrator of the Office of Electronic Government a report of the source code of the agency to which an exemption under paragraph (1) or (2) of subsection (a) applied during the fiscal year ending on September 30 of that year with a brief narrative justification of each exemption.

''(2) ANNUAL REPORT TO CONGRESS.—Not later than 1 year after the date of enactment of this Act [Dec. 23, 2024], and annually thereafter, the Administrator of

the Office of Electronic Government shall submit to the appropriate congressional committees a report on all exemptions granted under paragraph (1) or (2) of subsection (a) by each agency, including a compilation of all information, including the narrative justification, relating to each such exemption.

''(3) FORM.—The reports under paragraphs (1) and (2) shall be submitted in unclassified form, with a classified annex as appropriate.

''SEC. 5. GAO REPORT.

''Not later than 2 years after the date of enactment of this Act [Dec. 23, 2024], the Comptroller General of the United States shall submit to Congress a report that includes an assessment of the implementation of this Act.

''SEC. 6. RULE OF CONSTRUCTION.

''Nothing in this Act may be construed as requiring the disclosure of information or records that are exempt from public disclosure under section 552 of title 5, United States Code (commonly known as the 'Freedom of Information Act').

''SEC. 7. APPLICATION.

''This Act shall apply to custom-developed code that is developed or revised—

''(1) by a Federal employee not less than 180 days after the date of enactment of this Act [Dec. 23, 2024]; or

''(2) under a contract awarded pursuant to a solicitation issued not less than 180 days after the date of enactment of this Act.

''SEC. 8. REVISION OF FEDERAL ACQUISITION REGULATION.

''Not later than 1 year after the date of enactment of this Act [Dec. 23, 2024], the Federal Acquisition Regulation shall be revised as necessary to implement the provisions of this Act.

''SEC. 9. NO ADDITIONAL FUNDING.

''No additional funds are authorized to be appropriated to carry out this Act.''

IMPLEMENTATION OF TECHNOLOGY FOR CLASSIFICATION AND DECLASSIFICATION

Pub. L. 118–31, div. G, title VI, § 7605, Dec. 22, 2023, 137 Stat. 1098, provided that:

''(a) IN GENERAL.—Not later than 1 year after the date of the enactment of this Act [Dec. 22, 2023], the Administrator of the Office of Electronic Government (in this section referred to as the 'Administrator') shall, in consultation with the Secretary of Defense, the Director of the Central Intelligence Agency, the Director of National Intelligence, the Public Interest Declassification Board, the Director of the Information Security Oversight Office, and the head of the National Declassification Center of the National Archives and Records Administration—

''(1) research a technology-based solutions [sic]—

''(A) to support efficient and effective systems for classification and declassification; and

''(B) to be implemented on an interoperable and federated basis across the Federal Government; and

''(2) submit to the President and Congress, including the congressional intelligence committees [Select Committee on Intelligence of the Senate and Permanent Select Committee on Intelligence of the House of Representatives], the Committee on Armed Services, the Committee on Homeland Security and Governmental Affairs, the Committee on Foreign Relations, the Committee on the Judiciary of the Senate, and the Committee on Armed Services, the Committee on Oversight and Accountability, the Committee on Foreign Affairs, and the Committee on the Judiciary of the House of Representatives, recommendations regarding a technology-based solutions [sic] described in paragraph (1).

''(b) REPORT.—Not later than 540 days after the date of the enactment of this Act, the President shall submit to Congress a classified report describing actions taken to implement the recommendations under subsection (a)(2).''

21ST CENTURY INTEGRATED DIGITAL EXPERIENCE

Pub. L. 115–336, Dec. 20, 2018, 132 Stat. 5025, provided that:

''SECTION 1. SHORT TITLE.

''This Act may be cited as the '21st Century Integrated Digital Experience Act' or the '21st Century IDEA'.

''SEC. 2. DEFINITIONS.

''In this Act:

''(1) DIRECTOR.—The term 'Director' means the Director of the Office of Management and Budget.

''(2) EXECUTIVE AGENCY.—The term 'executive agency' has the meaning given the term 'Executive agency' in section 105 of title 5, United States Code.

''SEC. 3. WEBSITE MODERNIZATION.

''(a) REQUIREMENTS FOR NEW WEBSITES AND DIGITAL SERVICES.—Not later than 180 days after the date of enactment of this Act [Dec. 20, 2018], an executive agency that creates a website or digital service that is intended for use by the public, or conducts a redesign of an existing legacy website or digital service that is intended for use by the public, shall ensure to the greatest extent practicable that any new or redesigned website, web-based form, web-based application, or digital service—

''(1) is accessible to individuals with disabilities in accordance with section 508 of the Rehabilitation Act of 1973 (29 U.S.C. 794d);

''(2) has a consistent appearance;

''(3) does not overlap with or duplicate any legacy websites and, if applicable, ensure that legacy websites are regularly reviewed, eliminated, and consolidated;

''(4) contains a search function that allows users to easily search content intended for public use;

''(5) is provided through an industry standard secure connection;

''(6) is designed around user needs with data-driven analysis influencing management and development decisions, using qualitative and quantitative data to determine user goals, needs, and behaviors, and continually test the website, web-based form, web-based application, or digital service to ensure that user needs are addressed;

''(7) provides users of the new or redesigned website, web-based form, web-based application, or digital service with the option for a more customized digital experience that allows users to complete digital transactions in an efficient and accurate manner; and

''(8) is fully functional and usable on common mobile devices.

''(b) REQUIREMENTS FOR EXISTING EXECUTIVE AGENCY WEBSITES AND DIGITAL SERVICES.—Not later than 1 year after the date of enactment of this Act, the head of each executive agency that maintains a website or digital service that is made available to the public shall—

''(1) review each website or digital service; and

''(2) submit to Congress a report that includes—

''(A) a list of the websites and digital services maintained by the executive agency that are most viewed or utilized by the public or are otherwise important for public engagement;

''(B) from among the websites and digital services listed under subparagraph (A), a prioritization of websites and digital services that require modernization to meet the requirements under subsection (a); and

''(C) an estimation of the cost and schedule of modernizing the websites and digital services prioritized under subparagraph (B).

''(c) INTERNAL DIGITAL SERVICES.—The head of each executive agency shall ensure, to the greatest extent practicable, that any Intranet established after the date of enactment of this Act conforms to the requirements described in subsection (a).

''(d) PUBLIC REPORTING.—Not later than 1 year after the date of enactment of this Act and every year thereafter for 4 years, the head of each executive agency shall—

''(1) report annually to the Director on the progress of the executive agency in implementing the requirements described in this section for the previous year; and

''(2) include the information described in paragraph (1) in a publicly available report that is required under another provision of law.

''(e) COMPLIANCE WITH UNITED STATES WEBSITE STANDARDS.—Any website of an executive agency that is made available to the public after the date of enactment of this Act shall be in compliance with the website standards of the Technology Transformation Services of the General Services Administration.

''SEC. 4. DIGITIZATION OF GOVERNMENT SERVICES AND FORMS.

''(a) NON-DIGITAL SERVICES.—Not later than 180 days after the date of enactment of this Act [Dec. 20, 2018], the Director shall issue guidance to the head of each executive agency that establishes a process for the executive agency to—

''(1) identify public non-digital, paper-based, or in-person Government services; and

''(2) include in the budget request of the executive agency—

''(A) a list of non-digital services with the greatest impact that could be made available to the public through an online, mobile-friendly, digital service option in a manner that decreases cost, increases digital conversion rates, and improves customer experience; and

''(B) an estimation of the cost and schedule associated with carrying out the modernization described in subparagraph (A).

''(b) SERVICES REQUIRED TO BE DIGITAL.—The head of each executive agency shall regularly review public-facing applications and services to ensure that those applications and services are, to the greatest extent practicable, made available to the public in a digital format.

''(c) FORMS REQUIRED TO BE DIGITAL.—Not later than 2 years after the enactment of this Act, the head of each executive agency shall ensure that any paper based form that is related to serving the public is made available in a digital format that meets the requirements described in section 3(a).

''(d) NON-DIGITIZABLE PROCESSES.—If the head of an executive agency cannot make available in a digital format under this section an in-person Government service, form, or paper-based process, the head of the executive agency shall document—

''(1) the title of the in-person Government service, form, or paper-based process;

''(2) a description of the in-person Government service, form, or paper-based process;

''(3) each unit responsible for the in-person Government service, form, or paper-based process and the location of each unit in the organizational hierarchy of the executive agency;

''(4) any reasons why the in-person Government service, form, or paper-based process cannot be made available under this section; and

''(5) any potential solutions that could allow the in-person Government service, form, or paper-based process to be made available under this section, including the implementation of existing technologies, procedural changes, regulatory changes, and legislative changes.

''(e) PHYSICAL AVAILABILITY.—Each executive agency shall maintain an accessible method of completing digital services through in-person, paper-based, or other means, such that individuals without the ability to use digital services are not deprived of or impeded in access to those digital services.

''SEC. 5. ELECTRONIC SIGNATURES.

''Not later than 180 days after the date of the enactment of this Act, the head of each executive agency shall submit to the Director and the appropriate congressional committees a plan to accelerate the use of electronic signatures standards established under the Electronic Signatures in Global and National Commerce Act (15 U.S.C. 7001 et seq.).

''SEC. 6. CUSTOMER EXPERIENCE AND DIGITAL SERVICE DELIVERY.

''The Chief Information Officer of each executive agency, or a designee, shall—

''(1) coordinate and ensure alignment of the internal and external customer experience programs and strategy of the executive agency;

''(2) coordinate with the management leaders of the executive agency, including the head of the executive agency, the Chief Financial Officer, and any program manager, to ensure proper funding to support the implementation of this Act;

''(3) continually examine the digital service delivery strategy of the executive agency to the public and submit recommendations to the head of the executive agency providing guidance and best practices suitable to the mission of the executive agency;

''(4) using qualitative and quantitative data obtained from across the executive agency relating to the experience and satisfaction of customers, identify areas of concern that need improvement and improve the delivery of customer service;

''(5) coordinate and ensure, with the approval of the head of the executive agency, compliance by the executive agency with section 3559 of title 44, United States Code; and

''(6) to the extent practicable, coordinate with other agencies and seek to maintain as much standardization and commonality with other agencies as practicable in implementing the requirements of this Act, to best enable future transitions to centralized shared services.

''SEC. 7. STANDARDIZATION.

''(a) DESIGN AND IMPLEMENTATION.—Each executive agency shall, to the extent practicable, seek to maintain as much standardization and commonality with other executive agencies as practicable in implementing the requirements of this Act to best enable future transitions to centralized shared services.

''(b) COORDINATION.—The Chief Information Officer of each executive agency, or a designee, shall coordinate the implementation of the requirements of this Act, including the development of standards and commonalities.

''(c) FEDERAL SUPPLY SCHEDULE.—

''(1) IN GENERAL.—The General Services Administration shall make available under a Federal Supply Schedule the systems and services necessary to fulfill the requirements of this Act.

''(2) REQUIREMENTS.—The Federal Supply Schedule described in paragraph (1) shall, to the extent practicable, ensure interoperability between executive agencies, compliance with industry standards, and adherence to best practices for design, accessibility, and information security.''

FEDERAL MANAGEMENT AND PROMOTION OF ELECTRONIC GOVERNMENT SERVICES

Pub. L. 107–347, title II, Dec. 17, 2002, 116 Stat. 2910, as amended by Pub. L. 108–271, §8(b), July 7, 2004, 118 Stat. 814; Pub. L. 108–281, §1, Aug. 2, 2004, 118 Stat. 889, provided that:

''SEC. 201. DEFINITIONS.

''Except as otherwise provided, in this title the definitions under sections 3502 and 3601 of title 44, United States Code, shall apply.

''SEC. 202. FEDERAL AGENCY RESPONSIBILITIES.

''(a) IN GENERAL.—The head of each agency shall be responsible for—

''(1) complying with the requirements of this Act [see Tables for classification] (including the amendments made by this Act), the related information re-

source management policies and guidance established by the Director of the Office of Management and Budget, and the related information technology standards promulgated by the Secretary of Commerce;

''(2) ensuring that the information resource management policies and guidance established under this Act by the Director, and the related information technology standards promulgated by the Secretary of Commerce are communicated promptly and effectively to all relevant officials within their agency; and

''(3) supporting the efforts of the Director and the Administrator of the General Services Administration to develop, maintain, and promote an integrated Internet-based system of delivering Federal Government information and services to the public under section 204.

''(b) PERFORMANCE INTEGRATION.—

''(1) Agencies shall develop performance measures that demonstrate how electronic government enables progress toward agency objectives, strategic goals, and statutory mandates.

''(2) In measuring performance under this section, agencies shall rely on existing data collections to the extent practicable.

''(3) Areas of performance measurement that agencies should consider include—

''(A) customer service;

''(B) agency productivity; and

''(C) adoption of innovative information technology, including the appropriate use of commercial best practices.

''(4) Agencies shall link their performance goals, as appropriate, to key groups, including citizens, businesses, and other governments, and to internal Federal Government operations.

''(5) As appropriate, agencies shall work collectively in linking their performance goals to groups identified under paragraph (4) and shall use information technology in delivering Government information and services to those groups.

''(c) AVOIDING DIMINISHED ACCESS.—When promulgating policies and implementing programs regarding the provision of Government information and services over the Internet, agency heads shall consider the impact on persons without access to the Internet, and shall, to the extent practicable—

''(1) ensure that the availability of Government information and services has not been diminished for individuals who lack access to the Internet; and

''(2) pursue alternate modes of delivery that make Government information and services more accessible to individuals who do not own computers or lack access to the Internet.

''(d) ACCESSIBILITY TO PEOPLE WITH DISABILITIES.—All actions taken by Federal departments and agencies under this Act [see Tables for classification] shall be in compliance with section 508 of the Rehabilitation Act of 1973 (29 U.S.C. 794d).

''(e) SPONSORED ACTIVITIES.—Agencies shall sponsor activities that use information technology to engage the public in the development and implementation of policies and programs.

''(f) CHIEF INFORMATION OFFICERS.—The Chief Information Officer of each of the agencies designated under chapter 36 of title 44, United States Code (as added by this Act) shall be responsible for—

''(1) participating in the functions of the Chief Information Officers Council; and

''(2) monitoring the implementation, within their respective agencies, of information technology standards promulgated by the Secretary of Commerce, including common standards for interconnectivity and interoperability, categorization of Federal Government electronic information, and computer system efficiency and security.

''(g) E-GOVERNMENT STATUS REPORT.—

''(1) IN GENERAL.—Each agency shall compile and submit to the Director an annual E-Government Status Report on—

''(A) the status of the implementation by the agency of electronic government initiatives;

''(B) compliance by the agency with this Act [see Tables for classification]; and

''(C) how electronic Government initiatives of the agency improve performance in delivering programs to constituencies.

''(2) SUBMISSION.—Each agency shall submit an annual report under this subsection—

''(A) to the Director at such time and in such manner as the Director requires;

''(B) consistent with related reporting requirements; and

''(C) which addresses any section in this title relevant to that agency.

''(h) USE OF TECHNOLOGY.—Nothing in this Act [see Tables for classification] supersedes the responsibility of an agency to use or manage information technology to deliver Government information and services that fulfill the statutory mission and programs of the agency.

''(i) NATIONAL SECURITY SYSTEMS.—

''(1) INAPPLICABILITY.—Except as provided under paragraph (2), this title does not apply to national security systems as defined in section 11103 of title 40, United States Code.

''(2) APPLICABILITY.—This section, section 203, and section 214 do apply to national security systems to the extent practicable and consistent with law.

''SEC. 203. COMPATIBILITY OF EXECUTIVE AGENCY METHODS FOR USE AND ACCEPTANCE OF ELECTRONIC SIGNATURES.

''(a) PURPOSE.—The purpose of this section is to achieve interoperable implementation of electronic signatures for appropriately secure electronic transactions with Government.

''(b) ELECTRONIC SIGNATURES.—In order to fulfill the objectives of the Government Paperwork Elimination Act (Public Law 105–277; 112 Stat. 2681–749 through 2681–751) [44 U.S.C. 3504 note], each Executive agency (as defined under section 105 of title 5, United States Code) shall ensure that its methods for use and acceptance of electronic signatures are compatible with the relevant policies and procedures issued by the Director.

''(c) AUTHORITY FOR ELECTRONIC SIGNATURES.—The Administrator of General Services shall support the Director by establishing a framework to allow efficient interoperability among Executive agencies when using electronic signatures, including processing of digital signatures.

''(d) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated to the General Services Administration, to ensure the development and operation of a Federal bridge certification authority for digital signature compatibility, and for other activities consistent with this section, $8,000,000 or such sums as are necessary in fiscal year 2003, and such sums as are necessary for each fiscal year thereafter.

''SEC. 204. FEDERAL INTERNET PORTAL.

''(a) IN GENERAL.—

''(1) PUBLIC ACCESS.—The Director shall work with the Administrator of the General Services Administration and other agencies to maintain and promote an integrated Internet-based system of providing the public with access to Government information and services.

''(2) CRITERIA.—To the extent practicable, the integrated system shall be designed and operated according to the following criteria:

''(A) The provision of Internet-based Government information and services directed to key groups, including citizens, business, and other governments, and integrated according to function or topic rather than separated according to the boundaries of agency jurisdiction.

''(B) An ongoing effort to ensure that Internet-based Government services relevant to a given citizen activity are available from a single point.

''(C) Access to Federal Government information and services consolidated, as appropriate, with

Internet-based information and services provided by State, local, and tribal governments.

''(D) Access to Federal Government information held by 1 or more agencies shall be made available in a manner that protects privacy, consistent with law.

''(b) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated to the General Services Administration $15,000,000 for the maintenance, improvement, and promotion of the integrated Internet-based system for fiscal year 2003, and such sums as are necessary for fiscal years 2004 through 2007.

''SEC. 205. FEDERAL COURTS.

''(a) INDIVIDUAL COURT WEBSITES.—The Chief Justice of the United States, the chief judge of each circuit and district and of the Court of Federal Claims, and the chief bankruptcy judge of each district shall cause to be established and maintained, for the court of which the judge is chief justice or judge, a website that contains the following information or links to websites with the following information:

''(1) Location and contact information for the courthouse, including the telephone numbers and contact names for the clerk's office and justices' or judges' chambers.

''(2) Local rules and standing or general orders of the court.

''(3) Individual rules, if in existence, of each justice or judge in that court.

''(4) Access to docket information for each case.

''(5) Access to the substance of all written opinions issued by the court, regardless of whether such opinions are to be published in the official court reporter, in a text searchable format.

''(6) Access to documents filed with the courthouse in electronic form, to the extent provided under subsection (c).

''(7) Any other information (including forms in a format that can be downloaded) that the court determines useful to the public.

''(b) MAINTENANCE OF DATA ONLINE.—

''(1) UPDATE OF INFORMATION.—The information and rules on each website shall be updated regularly and kept reasonably current.

''(2) CLOSED CASES.—Electronic files and docket information for cases closed for more than 1 year are not required to be made available online, except all written opinions with a date of issuance after the effective date of this section [see Effective Date note set out under section 3601 of this title] shall remain available online.

''(c) ELECTRONIC FILINGS.—

''(1) IN GENERAL.—Except as provided under paragraph (2) or in the rules prescribed under paragraph (3), each court shall make any document that is filed electronically publicly available online. A court may convert any document that is filed in paper form to electronic form. To the extent such conversions are made, all such electronic versions of the document shall be made available online.

''(2) EXCEPTIONS.—Documents that are filed that are not otherwise available to the public, such as documents filed under seal, shall not be made available online.

''(3) PRIVACY AND SECURITY CONCERNS.—

''(A)(i) The Supreme Court shall prescribe rules, in accordance with sections 2072 and 2075 of title 28, United States Code, to protect privacy and security concerns relating to electronic filing of documents and the public availability under this subsection of documents filed electronically or converted to electronic form.

''(ii) Such rules shall provide to the extent practicable for uniform treatment of privacy and security issues throughout the Federal courts.

''(iii) Such rules shall take into consideration best practices in Federal and State courts to protect private information or otherwise maintain necessary information security.

''(iv) Except as provided in clause (v), to the extent that such rules provide for the redaction of certain categories of information in order to protect privacy and security concerns, such rules shall provide that a party that wishes to file an otherwise proper document containing such protected information may file an unredacted document under seal, which shall be retained by the court as part of the record, and which, at the discretion of the court and subject to any applicable rules issued in accordance with chapter 131 of title 28, United States Code, shall be either in lieu of, or in addition to, a redacted copy in the public file.

''(v) Such rules may require the use of appropriate redacted identifiers in lieu of protected information described in clause (iv) in any pleading, motion, or other paper filed with the court (except with respect to a paper that is an exhibit or other evidentiary matter, or with respect to a reference list described in this subclause), or in any written discovery response—

''(I) by authorizing the filing under seal, and permitting the amendment as of right under seal, of a reference list that—

''(aa) identifies each item of unredacted protected information that the attorney or, if there is no attorney, the party, certifies is relevant to the case; and

''(bb) specifies an appropriate redacted identifier that uniquely corresponds to each item of unredacted protected information listed; and

''(II) by providing that all references in the case to the redacted identifiers in such reference list shall be construed, without more, to refer to the corresponding unredacted item of protected information.

''(B)(i) Subject to clause (ii), the Judicial Conference of the United States may issue interim rules, and interpretive statements relating to the application of such rules, which conform to the requirements of this paragraph and which shall cease to have effect upon the effective date of the rules required under subparagraph (A).

''(ii) Pending issuance of the rules required under subparagraph (A), any rule or order of any court, or of the Judicial Conference, providing for the redaction of certain categories of information in order to protect privacy and security concerns arising from electronic filing or electronic conversion shall comply with, and be construed in conformity with, subparagraph (A)(iv).

''(C) Not later than 1 year after the rules prescribed under subparagraph (A) take effect, and every 2 years thereafter, the Judicial Conference shall submit to Congress a report on the adequacy of those rules to protect privacy and security.

''(d) DOCKETS WITH LINKS TO DOCUMENTS.—The Judicial Conference of the United States shall explore the feasibility of technology to post online dockets with links allowing all filings, decisions, and rulings in each case to be obtained from the docket sheet of that case.

''(e) COST OF PROVIDING ELECTRONIC DOCKETING INFORMATION.—[Amended section 303(a) of Pub. L. 102–140, set out as a note under section 1913 of Title 28, Judiciary and Judicial Procedure.]

''(f) TIME REQUIREMENTS.—Not later than 2 years after the effective date of this title [see Effective Date note set out under section 3601 of this title], the websites under subsection (a) shall be established, except that access to documents filed in electronic form shall be established not later than 4 years after that effective date.

''(g) DEFERRAL.—

''(1) IN GENERAL.—

''(A) ELECTION.—

''(i) NOTIFICATION.—The Chief Justice of the United States, a chief judge, or chief bankruptcy judge may submit a notification to the Administrative Office of the United States Courts to defer compliance with any requirement of this section

with respect to the Supreme Court, a court of appeals, district, or the bankruptcy court of a district.

''(ii) CONTENTS.—A notification submitted under this subparagraph shall state—

''(I) the reasons for the deferral; and

''(II) the online methods, if any, or any alternative methods, such court or district is using to provide greater public access to information.

''(B) EXCEPTION.—To the extent that the Supreme Court, a court of appeals, district, or bankruptcy court of a district maintains a website under subsection (a), the Supreme Court or that court of appeals or district shall comply with subsection (b)(1).

''(2) REPORT.—Not later than 1 year after the effective date of this title [see Effective Date note set out under section 3601 of this title], and every year thereafter, the Judicial Conference of the United States shall submit a report to the Committees on Governmental Affairs and the Judiciary of the Senate and the Committees on Government Reform [now Committee on Oversight and Accountability] and the Judiciary of the House of Representatives that—

''(A) contains all notifications submitted to the Administrative Office of the United States Courts under this subsection; and

''(B) summarizes and evaluates all notifications.

''SEC. 206. REGULATORY AGENCIES.

''(a) PURPOSES.—The purposes of this section are to—

''(1) improve performance in the development and issuance of agency regulations by using information technology to increase access, accountability, and transparency; and

''(2) enhance public participation in Government by electronic means, consistent with requirements under subchapter II of chapter 5 of title 5, United States Code, (commonly referred to as the 'Administrative Procedures Act').

''(b) INFORMATION PROVIDED BY AGENCIES ONLINE.—To the extent practicable as determined by the agency in consultation with the Director, each agency (as defined under section 551 of title 5, United States Code) shall ensure that a publicly accessible Federal Government website includes all information about that agency required to be published in the Federal Register under paragraphs (1) and (2) of section 552(a) of title 5, United States Code.

''(c) SUBMISSIONS BY ELECTRONIC MEANS.—To the extent practicable, agencies shall accept submissions under section 553(c) of title 5, United States Code, by electronic means.

''(d) ELECTRONIC DOCKETING.—

''(1) IN GENERAL.—To the extent practicable, as determined by the agency in consultation with the Director, agencies shall ensure that a publicly accessible Federal Government website contains electronic dockets for rulemakings under section 553 of title 5, United States Code.

''(2) INFORMATION AVAILABLE.—Agency electronic dockets shall make publicly available online to the extent practicable, as determined by the agency in consultation with the Director—

''(A) all submissions under section 553(c) of title 5, United States Code; and

''(B) other materials that by agency rule or practice are included in the rulemaking docket under section 553(c) of title 5, United States Code, whether or not submitted electronically.

''(e) TIME LIMITATION.—Agencies shall implement the requirements of this section consistent with a timetable established by the Director and reported to Congress in the first annual report under section 3606 of title 44 (as added by this Act).

''SEC. 207. ACCESSIBILITY, USABILITY, AND PRESERVATION OF GOVERNMENT INFORMATION.

''(a) PURPOSE.—The purpose of this section is to improve the methods by which Government information, including information on the Internet, is organized, preserved, and made accessible to the public.

''(b) DEFINITIONS.—In this section, the term—

''(1) 'Committee' means the Interagency Committee on Government Information established under subsection (c); and

''(2) 'directory' means a taxonomy of subjects linked to websites that—

''(A) organizes Government information on the Internet according to subject matter; and

''(B) may be created with the participation of human editors.

''(c) INTERAGENCY COMMITTEE.—

''(1) ESTABLISHMENT.—Not later than 180 days after the date of enactment of this title [Dec. 17, 2002], the Director shall establish the Interagency Committee on Government Information.

''(2) MEMBERSHIP.—The Committee shall be chaired by the Director or the designee of the Director and—

''(A) shall include representatives from—

''(i) the National Archives and Records Administration;

''(ii) the offices of the Chief Information Officers from Federal agencies; and

''(iii) other relevant officers from the executive branch; and

''(B) may include representatives from the Federal legislative and judicial branches.

''(3) FUNCTIONS.—The Committee shall—

''(A) engage in public consultation to the maximum extent feasible, including consultation with interested communities such as public advocacy organizations;

''(B) conduct studies and submit recommendations, as provided under this section, to the Director and Congress; and

''(C) share effective practices for access to, dissemination of, and retention of Federal information.

''(4) TERMINATION.—The Committee may be terminated on a date determined by the Director, except the Committee may not terminate before the Committee submits all recommendations required under this section.

''(d) CATEGORIZING OF INFORMATION.—

''(1) COMMITTEE FUNCTIONS.—Not later than 2 years after the date of enactment of this Act [Dec. 17, 2002], the Committee shall submit recommendations to the Director on—

''(A) the adoption of standards, which are open to the maximum extent feasible, to enable the organization and categorization of Government information—

''(i) in a way that is searchable electronically, including by searchable identifiers; and

''(ii) in ways that are interoperable across agencies;

''(B) the definition of categories of Government information which should be classified under the standards; and

''(C) determining priorities and developing schedules for the initial implementation of the standards by agencies.

''(2) FUNCTIONS OF THE DIRECTOR.—Not later than 1 year after the submission of recommendations under paragraph (1), the Director shall issue policies—

''(A) requiring that agencies use standards, which are open to the maximum extent feasible, to enable the organization and categorization of Government information—

''(i) in a way that is searchable electronically, including by searchable identifiers;

''(ii) in ways that are interoperable across agencies; and

''(iii) that are, as appropriate, consistent with the provisions under section 3602(f)(8) of title 44, United States Code;

''(B) defining categories of Government information which shall be required to be classified under the standards; and

''(C) determining priorities and developing schedules for the initial implementation of the standards by agencies.

''(3) MODIFICATION OF POLICIES.—After the submission of agency reports under paragraph (4), the Director shall modify the policies, as needed, in consultation with the Committee and interested parties.

''(4) AGENCY FUNCTIONS.—Each agency shall report annually to the Director, in the report established under section 202(g), on compliance of that agency with the policies issued under paragraph (2)(A).

''(e) PUBLIC ACCESS TO ELECTRONIC INFORMATION.—

''(1) COMMITTEE FUNCTIONS.—Not later than 2 years after the date of enactment of this Act [Dec. 17, 2002], the Committee shall submit recommendations to the Director and the Archivist of the United States on—

''(A) the adoption by agencies of policies and procedures to ensure that chapters 21, 25, 27, 29, and 31 of title 44, United States Code, are applied effectively and comprehensively to Government information on the Internet and to other electronic records; and

''(B) the imposition of timetables for the implementation of the policies and procedures by agencies.

''(2) FUNCTIONS OF THE ARCHIVIST.—Not later than 1 year after the submission of recommendations by the Committee under paragraph (1), the Archivist of the United States shall issue policies—

''(A) requiring the adoption by agencies of policies and procedures to ensure that chapters 21, 25, 27, 29, and 31 of title 44, United States Code, are applied effectively and comprehensively to Government information on the Internet and to other electronic records; and

''(B) imposing timetables for the implementation of the policies, procedures, and technologies by agencies.

''(3) MODIFICATION OF POLICIES.—After the submission of agency reports under paragraph (4), the Archivist of the United States shall modify the policies, as needed, in consultation with the Committee and interested parties.

''(4) AGENCY FUNCTIONS.—Each agency shall report annually to the Director, in the report established under section 202(g), on compliance of that agency with the policies issued under paragraph (2)(A).

''(f) AGENCY WEBSITES.—

''(1) STANDARDS FOR AGENCY WEBSITES.—Not later than 2 years after the effective date of this title [see Effective Date note set out under section 3601 of this title], the Director shall promulgate guidance for agency websites that includes—

''(A) requirements that websites include direct links to—

''(i) descriptions of the mission and statutory authority of the agency;

''(ii) information made available to the public under subsections (a)(1) and (b) of section 552 of title 5, United States Code (commonly referred to as the 'Freedom of Information Act');

''(iii) information about the organizational structure of the agency; and

''(iv) the strategic plan of the agency developed under section 306 of title 5, United States Code; and

''(B) minimum agency goals to assist public users to navigate agency websites, including—

''(i) speed of retrieval of search results;

''(ii) the relevance of the results;

''(iii) tools to aggregate and disaggregate data; and

''(iv) security protocols to protect information.

''(2) AGENCY REQUIREMENTS.—(A) Not later than 2 years after the date of enactment of this Act [Dec. 17, 2002], each agency shall—

''(i) consult with the Committee and solicit public comment;

''(ii) establish a process for determining which Government information the agency intends to make available and accessible to the public on the Internet and by other means;

''(iii) develop priorities and schedules for making Government information available and accessible;

''(iv) make such final determinations, priorities, and schedules available for public comment;

''(v) post such final determinations, priorities, and schedules on the Internet; and

''(vi) submit such final determinations, priorities, and schedules to the Director, in the report established under section 202(g).

''(B) Each agency shall update determinations, priorities, and schedules of the agency, as needed, after consulting with the Committee and soliciting public comment, if appropriate.

''(3) PUBLIC DOMAIN DIRECTORY OF PUBLIC FEDERAL GOVERNMENT WEBSITES.—

''(A) ESTABLISHMENT.—Not later than 2 years after the effective date of this title [see Effective Date note set out under section 3601 of this title], the Director and each agency shall—

''(i) develop and establish a public domain directory of public Federal Government websites; and

''(ii) post the directory on the Internet with a link to the integrated Internet-based system established under section 204.

''(B) DEVELOPMENT.—With the assistance of each agency, the Director shall—

''(i) direct the development of the directory through a collaborative effort, including input from—

''(I) agency librarians;

''(II) information technology managers;

''(III) program managers;

''(IV) records managers;

''(V) Federal depository librarians; and

''(VI) other interested parties; and

''(ii) develop a public domain taxonomy of subjects used to review and categorize public Federal Government websites.

''(C) UPDATE.—With the assistance of each agency, the Administrator of the Office of Electronic Government shall—

''(i) update the directory as necessary, but not less than every 6 months; and

''(ii) solicit interested persons for improvements to the directory.

''(g) ACCESS TO FEDERALLY FUNDED RESEARCH AND DEVELOPMENT.—

''(1) DEVELOPMENT AND MAINTENANCE OF GOVERNMENTWIDE REPOSITORY AND WEBSITE.—

''(A) REPOSITORY AND WEBSITE.—The Director of the Office of Management and Budget (or the Director's delegate), in consultation with the Director of the Office of Science and Technology Policy and other relevant agencies, shall ensure the development and maintenance of—

''(i) a repository that fully integrates, to the maximum extent feasible, information about research and development funded by the Federal Government, and the repository shall—

''(I) include information about research and development funded by the Federal Government, consistent with any relevant protections for the information under section 552 of title 5, United States Code, and performed by—

''(aa) institutions not a part of the Federal Government, including State, local, and foreign governments; industrial firms; educational institutions; not-for-profit organizations; federally funded research and development centers; and private individuals; and

''(bb) entities of the Federal Government, including research and development laboratories, centers, and offices; and

''(II) integrate information about each separate research and development task or award, including—

''(aa) the dates upon which the task or award is expected to start and end;

''(bb) a brief summary describing the objective and the scientific and technical focus of the task or award;

''(cc) the entity or institution performing the task or award and its contact information;

''(dd) the total amount of Federal funds expected to be provided to the task or award over its lifetime and the amount of funds expected to be provided in each fiscal year in which the work of the task or award is ongoing;

''(ee) any restrictions attached to the task or award that would prevent the sharing with the general public of any or all of the information required by this subsection, and the reasons for such restrictions; and

''(ff) such other information as may be determined to be appropriate; and

''(ii) 1 or more websites upon which all or part of the repository of Federal research and development shall be made available to and searchable by Federal agencies and non-Federal entities, including the general public, to facilitate—

''(I) the coordination of Federal research and development activities;

''(II) collaboration among those conducting Federal research and development;

''(III) the transfer of technology among Federal agencies and between Federal agencies and non-Federal entities; and

''(IV) access by policymakers and the public to information concerning Federal research and development activities.

''(B) OVERSIGHT.—The Director of the Office of Management and Budget shall issue any guidance determined necessary to ensure that agencies provide all information requested under this subsection.

''(2) AGENCY FUNCTIONS.—Any agency that funds Federal research and development under this subsection shall provide the information required to populate the repository in the manner prescribed by the Director of the Office of Management and Budget.

''(3) COMMITTEE FUNCTIONS.—Not later than 18 months after the date of enactment of this Act [Dec. 17, 2002], working with the Director of the Office of Science and Technology Policy, and after consultation with interested parties, the Committee shall submit recommendations to the Director on—

''(A) policies to improve agency reporting of information for the repository established under this subsection; and

''(B) policies to improve dissemination of the results of research performed by Federal agencies and federally funded research and development centers.

''(4) FUNCTIONS OF THE DIRECTOR.—After submission of recommendations by the Committee under paragraph (3), the Director shall report on the recommendations of the Committee and Director to Congress, in the E-Government report under section 3606 of title 44 (as added by this Act).

''(5) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated for the development, maintenance, and operation of the Governmentwide repository and website under this subsection—

''(A) $2,000,000 in each of the fiscal years 2003 through 2005; and

''(B) such sums as are necessary in each of the fiscal years 2006 and 2007.

''SEC. 208. PRIVACY PROVISIONS.

''(a) PURPOSE.—The purpose of this section is to ensure sufficient protections for the privacy of personal information as agencies implement citizen-centered electronic Government.

''(b) PRIVACY IMPACT ASSESSMENTS.—

''(1) RESPONSIBILITIES OF AGENCIES.—

''(A) IN GENERAL.—An agency shall take actions described under subparagraph (B) before—

''(i) developing or procuring information technology that collects, maintains, or disseminates information that is in an identifiable form; or

''(ii) initiating a new collection of information that—

''(I) will be collected, maintained, or disseminated using information technology; and

''(II) includes any information in an identifiable form permitting the physical or online contacting of a specific individual, if identical questions have been posed to, or identical reporting requirements imposed on, 10 or more persons, other than agencies, instrumentalities, or employees of the Federal Government.

''(B) AGENCY ACTIVITIES.—To the extent required under subparagraph (A), each agency shall—

''(i) conduct a privacy impact assessment;

''(ii) ensure the review of the privacy impact assessment by the Chief Information Officer, or equivalent official, as determined by the head of the agency; and

''(iii) if practicable, after completion of the review under clause (ii), make the privacy impact assessment publicly available through the website of the agency, publication in the Federal Register, or other means.

''(C) SENSITIVE INFORMATION.—Subparagraph (B)(iii) may be modified or waived for security reasons, or to protect classified, sensitive, or private information contained in an assessment.

''(D) COPY TO DIRECTOR.—Agencies shall provide the Director with a copy of the privacy impact assessment for each system for which funding is requested.

''(2) CONTENTS OF A PRIVACY IMPACT ASSESSMENT.—

''(A) IN GENERAL.—The Director shall issue guidance to agencies specifying the required contents of a privacy impact assessment.

''(B) GUIDANCE.—The guidance shall—

''(i) ensure that a privacy impact assessment is commensurate with the size of the information system being assessed, the sensitivity of information that is in an identifiable form in that system, and the risk of harm from unauthorized release of that information; and

''(ii) require that a privacy impact assessment address—

''(I) what information is to be collected;

''(II) why the information is being collected;

''(III) the intended use of the agency of the information;

''(IV) with whom the information will be shared;

''(V) what notice or opportunities for consent would be provided to individuals regarding what information is collected and how that information is shared;

''(VI) how the information will be secured; and

''(VII) whether a system of records is being created under section 552a of title 5, United States Code, (commonly referred to as the 'Privacy Act').

''(3) RESPONSIBILITIES OF THE DIRECTOR.—The Director shall—

''(A) develop policies and guidelines for agencies on the conduct of privacy impact assessments;

''(B) oversee the implementation of the privacy impact assessment process throughout the Government; and

''(C) require agencies to conduct privacy impact assessments of existing information systems or ongoing collections of information that is in an identifiable form as the Director determines appropriate.

''(c) PRIVACY PROTECTIONS ON AGENCY WEBSITES.—

''(1) PRIVACY POLICIES ON WEBSITES.—

''(A) GUIDELINES FOR NOTICES.—The Director shall develop guidance for privacy notices on agency websites used by the public.

''(B) CONTENTS.—The guidance shall require that a privacy notice address, consistent with section 552a of title 5, United States Code—

''(i) what information is to be collected;

''(ii) why the information is being collected;

''(iii) the intended use of the agency of the information;

''(iv) with whom the information will be shared;

''(v) what notice or opportunities for consent would be provided to individuals regarding what information is collected and how that information is shared;

''(vi) how the information will be secured; and

''(vii) the rights of the individual under section 552a of title 5, United States Code (commonly referred to as the 'Privacy Act'), and other laws relevant to the protection of the privacy of an individual.

''(2) PRIVACY POLICIES IN MACHINE-READABLE FORMATS.—The Director shall issue guidance requiring agencies to translate privacy policies into a standardized machine-readable format.

''(d) DEFINITION.—In this section, the term 'identifiable form' means any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means.

''SEC. 209. FEDERAL INFORMATION TECHNOLOGY WORKFORCE DEVELOPMENT.

''(a) PURPOSE.—The purpose of this section is to improve the skills of the Federal workforce in using information technology to deliver Government information and services.

''(b) WORKFORCE DEVELOPMENT.—

''(1) IN GENERAL.—In consultation with the Director of the Office of Management and Budget, the Chief Information Officers Council, and the Administrator of General Services, the Director of the Office of Personnel Management shall—

''(A) analyze, on an ongoing basis, the personnel needs of the Federal Government related to information technology and information resource management;

''(B) identify where current information technology and information resource management training do not satisfy the personnel needs described in subparagraph (A);

''(C) oversee the development of curricula, training methods, and training priorities that correspond to the projected personnel needs of the Federal Government related to information technology and information resource management; and

''(D) assess the training of Federal employees in information technology disciplines in order to ensure that the information resource management needs of the Federal Government are addressed.

''(2) INFORMATION TECHNOLOGY TRAINING PROGRAMS.—The head of each Executive agency, after consultation with the Director of the Office of Personnel Management, the Chief Information Officers Council, and the Administrator of General Services, shall establish and operate information technology training programs consistent with the requirements of this subsection. Such programs shall—

''(A) have curricula covering a broad range of information technology disciplines corresponding to the specific information technology and information resource management needs of the agency involved;

''(B) be developed and applied according to rigorous standards; and

''(C) be designed to maximize efficiency, through the use of self-paced courses, online courses, on-the-job training, and the use of remote instructors, wherever such features can be applied without reducing the effectiveness of the training or negatively impacting academic standards.

''(3) GOVERNMENTWIDE POLICIES AND EVALUATION.—The Director of the Office of Personnel Management, in coordination with the Director of the Office of Management and Budget, shall issue policies to promote the development of performance standards for training and uniform implementation of this subsection by Executive agencies, with due regard for differences in program requirements among agencies that may be appropriate and warranted in view of the agency mission. The Director of the Office of Personnel Management shall evaluate the implementation of the provisions of this subsection by Executive agencies.

''(4) CHIEF INFORMATION OFFICER AUTHORITIES AND RESPONSIBILITIES.—Subject to the authority, direction, and control of the head of an Executive agency, the chief information officer of such agency shall carry out all powers, functions, and duties of the head of the agency with respect to implementation of this subsection. The chief information officer shall ensure that the policies of the agency head established in accordance with this subsection are implemented throughout the agency.

''(5) INFORMATION TECHNOLOGY TRAINING REPORTING.—The Director of the Office of Management and Budget shall ensure that the heads of Executive agencies collect and maintain standardized information on the information technology and information resources management workforce related to the implementation of this subsection.

''(6) AUTHORITY TO DETAIL EMPLOYEES TO NON-FEDERAL EMPLOYERS.—In carrying out the preceding provisions of this subsection, the Director of the Office of Personnel Management may provide for a program under which a Federal employee may be detailed to a non-Federal employer. The Director of the Office of Personnel Management shall prescribe regulations for such program, including the conditions for service and duties as the Director considers necessary.

''(7) COORDINATION PROVISION.—An assignment described in section 3703 of title 5, United States Code, may not be made unless a program under paragraph (6) is established, and the assignment is made in accordance with the requirements of such program.

''(8) EMPLOYEE PARTICIPATION.—Subject to information resource management needs and the limitations imposed by resource needs in other occupational areas, and consistent with their overall workforce development strategies, agencies shall encourage employees to participate in occupational information technology training.

''(9) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated to the Office of Personnel Management for the implementation of this subsection, $15,000,000 in fiscal year 2003, and such sums as are necessary for each fiscal year thereafter.

''(10) EXECUTIVE AGENCY DEFINED.—For purposes of this subsection, the term 'Executive agency' has the meaning given the term 'agency' under section 3701 of title 5, United States Code (as added by subsection (c)).

''(c) INFORMATION TECHNOLOGY EXCHANGE PROGRAM.—

''(1) IN GENERAL.—[Enacted chapter 37 of Title 5, Government Organization and Employees.]

''(2) REPORT.—Not later than 4 years after the date of the enactment of this Act [Dec. 17, 2002], the Government Accountability Office shall prepare and submit to the Committee on Government Reform [now Committee on Oversight and Accountability] of the House of Representatives and the Committee on Governmental Affairs [now Committee on Homeland Security and Governmental Affairs] of the Senate a report on the operation of chapter 37 of title 5, United States Code (as added by this subsection). Such report shall include—

''(A) an evaluation of the effectiveness of the program established by such chapter; and

''(B) a recommendation as to whether such program should be continued (with or without modification) or allowed to lapse.

''(3) CLERICAL AMENDMENT.—[Amended analysis for part III of Title 5.]

''(d) ETHICS PROVISIONS.—

''(1) ONE-YEAR RESTRICTION ON CERTAIN COMMUNICATIONS.—[Amended section 207 of Title 18, Crimes and Criminal Procedure.]

''(2) DISCLOSURE OF CONFIDENTIAL INFORMATION.—[Amended section 1905 of Title 18.]

''(3) CONTRACT ADVICE.—[Amended section 207 of Title 18.]

''(4) RESTRICTION ON DISCLOSURE OF PROCUREMENT INFORMATION.—[Amended section 423 of Title 41, Public Contracts.]

''(e) REPORT ON EXISTING EXCHANGE PROGRAMS.—

''(1) EXCHANGE PROGRAM DEFINED.—For purposes of this subsection, the term 'exchange program' means an executive exchange program, the program under subchapter VI of chapter 33 of title 5, United States Code, and any other program which allows for—

''(A) the assignment of employees of the Federal Government to non-Federal employers;

''(B) the assignment of employees of non-Federal employers to the Federal Government; or

''(C) both.

''(2) REPORTING REQUIREMENT.—Not later than 1 year after the date of the enactment of this Act [Dec. 17, 2002], the Office of Personnel Management shall prepare and submit to the Committee on Government Reform [now Committee on Oversight and Accountability] of the House of Representatives and the Committee on Governmental Affairs [now Committee on Homeland Security and Governmental Affairs] of the Senate a report identifying all existing exchange programs.

''(3) SPECIFIC INFORMATION.—The report shall, for each such program, include—

''(A) a brief description of the program, including its size, eligibility requirements, and terms or conditions for participation;

''(B) specific citation to the law or other authority under which the program is established;

''(C) the names of persons to contact for more information, and how they may be reached; and

''(D) any other information which the Office considers appropriate.

''(f) REPORT ON THE ESTABLISHMENT OF A GOVERNMENTWIDE INFORMATION TECHNOLOGY TRAINING PROGRAM.—

''(1) IN GENERAL.—Not later January 1, 2003, the Office of Personnel Management, in consultation with the Chief Information Officers Council and the Administrator of General Services, shall review and submit to the Committee on Government Reform [now Committee on Oversight and Accountability] of the House of Representatives and the Committee on Governmental Affairs [now Committee on Homeland Security and Governmental Affairs] of the Senate a written report on the following:

''(A) The adequacy of any existing information technology training programs available to Federal employees on a Governmentwide basis.

''(B)(i) If one or more such programs already exist, recommendations as to how they might be improved.

''(ii) If no such program yet exists, recommendations as to how such a program might be designed and established.

''(C) With respect to any recommendations under subparagraph (B), how the program under chapter 37 of title 5, United States Code, might be used to help carry them out.

''(2) COST ESTIMATE.—The report shall, for any recommended program (or improvements) under paragraph (1)(B), include the estimated costs associated with the implementation and operation of such program as so established (or estimated difference in costs of any such program as so improved).

''(g) TECHNICAL AND CONFORMING AMENDMENTS.—

''(1) AMENDMENTS TO TITLE 5, UNITED STATES CODE.—[Amended sections 3111, 4108, and 7353 of Title 5.]

''(2) AMENDMENT TO TITLE 18, UNITED STATES CODE.—[Amended section 209 of Title 18.]

''(3) OTHER AMENDMENTS.—[Amended section 125(c)(1) of Pub. L. 100–238, set out as a note under section 8432 of Title 5.]

''SEC. 210. SHARE-IN-SAVINGS INITIATIVES.

''(a) DEFENSE CONTRACTS.—[Enacted former section 2332 of Title 10, Armed Forces.]

''(b) OTHER CONTRACTS.—[Enacted section 266a of Title 41.]

''(c) DEVELOPMENT OF INCENTIVES.—The Director of the Office of Management and Budget shall, in consultation with the Committee on Governmental Affairs [now Committee on Homeland Security and Governmental Affairs] of the Senate, the Committee on Government Reform [now Committee on Oversight and Accountability] of the House of Representatives, and executive agencies, develop techniques to permit an executive agency to retain a portion of the savings (after payment of the contractor's share of the savings) derived from share-in-savings contracts as funds are appropriated to the agency in future fiscal years.

''(d) REGULATIONS.—Not later than 270 days after the date of the enactment of this Act [Dec. 17, 2002], the Federal Acquisition Regulation shall be revised to implement the provisions enacted by this section. Such revisions shall—

''(1) provide for the use of competitive procedures in the selection and award of share-in-savings contracts to—

''(A) ensure the contractor's share of savings reflects the risk involved and market conditions; and

''(B) otherwise yield greatest value to the government; and

''(2) allow appropriate regulatory flexibility to facilitate the use of share-in-savings contracts by executive agencies, including the use of innovative provisions for technology refreshment and nonstandard Federal Acquisition Regulation contract clauses.

''(e) ADDITIONAL GUIDANCE.—The Administrator of General Services shall—

''(1) identify potential opportunities for the use of share-in-savings contracts; and

''(2) in consultation with the Director of the Office of Management and Budget, provide guidance to executive agencies for determining mutually beneficial savings share ratios and baselines from which savings may be measured.

''(f) OMB REPORT TO CONGRESS.—In consultation with executive agencies, the Director of the Office of Management and Budget shall, not later than 2 years after the date of the enactment of this Act [Dec. 17, 2002], submit to Congress a report containing—

''(1) a description of the number of share-in-savings contracts entered into by each executive agency under by [sic] this section and the amendments made by this section, and, for each contract identified—

''(A) the information technology acquired;

''(B) the total amount of payments made to the contractor; and

''(C) the total amount of savings or other measurable benefits realized;

''(2) a description of the ability of agencies to determine the baseline costs of a project against which savings can be measured; and

''(3) any recommendations, as the Director deems appropriate, regarding additional changes in law that may be necessary to ensure effective use of share-in-savings contracts by executive agencies.

''(g) GAO REPORT TO CONGRESS.—The Comptroller General shall, not later than 6 months after the report required under subsection (f) is submitted to Congress, conduct a review of that report and submit to Congress a report containing—

''(1) the results of the review;

''(2) an independent assessment by the Comptroller General of the effectiveness of the use of share-in-savings contracts in improving the mission-related and administrative processes of the executive agencies and the achievement of agency missions; and

''(3) a recommendation on whether the authority to enter into share-in-savings contracts should be continued.

''(h) REPEAL OF SHARE-IN-SAVINGS PILOT PROGRAM.—

''(1) REPEAL.—[Repealed section 11521 of Title 40, Public Buildings, Property, and Works.]

''(2) CONFORMING AMENDMENTS TO PILOT PROGRAM AUTHORITY.—[Amended sections 11501 to 11505 of Title 40.]

''(3) ADDITIONAL CONFORMING AMENDMENTS.—[Redesignated 11522 of Title 40 as 11521 and amended headings and analysis.]

''(i) DEFINITIONS.—In this section, the terms 'contractor', 'savings', and 'share-in-savings contract' have the meanings given those terms in section 317 of the Federal Property and Administrative Services Act of 1949 [former 41 U.S.C. 266a; now 41 U.S.C. note prec. 3901] (as added by subsection (b)).

''SEC. 211. AUTHORIZATION FOR ACQUISITION OF INFORMATION TECHNOLOGY BY STATE AND LOCAL GOVERNMENTS THROUGH FEDERAL SUPPLY SCHEDULES.

''(a) AUTHORITY TO USE CERTAIN SUPPLY SCHEDULES.—[Amended section 502 of Title 40.]

''(b) PROCEDURES.—Not later than 30 days after the date of the enactment of this Act [Dec. 17, 2002], the Administrator of General Services shall establish procedures to implement section 501(c) of title 40, United States Code (as added by subsection (a)).

''(c) REPORT.—Not later than December 31, 2004, the Administrator shall submit to the Committee on Government Reform [now Committee on Oversight and Accountability] of the House of Representatives and the Committee on Governmental Affairs [now Committee on Homeland Security and Governmental Affairs] of the Senate a report on the implementation and effects of the amendment made by subsection (a).

''SEC. 212. INTEGRATED REPORTING STUDY AND PILOT PROJECTS.

''(a) PURPOSES.—The purposes of this section are to—

''(1) enhance the interoperability of Federal information systems;

''(2) assist the public, including the regulated community, in electronically submitting information to agencies under Federal requirements, by reducing the burden of duplicate collection and ensuring the accuracy of submitted information; and

''(3) enable any person to integrate and obtain similar information held by 1 or more agencies under 1 or more Federal requirements without violating the privacy rights of an individual.

''(b) DEFINITIONS.—In this section, the term—

''(1) 'agency' means an Executive agency as defined under section 105 of title 5, United States Code; and

''(2) 'person' means any individual, trust, firm, joint stock company, corporation (including a government corporation), partnership, association, State, municipality, commission, political subdivision of a State, interstate body, or agency or component of the Federal Government.

''(c) REPORT.—

''(1) IN GENERAL.—Not later than 3 years after the date of enactment of this Act [Dec. 17, 2002], the Director shall oversee a study, in consultation with agencies, the regulated community, public interest organizations, and the public, and submit a report to the Committee on Governmental Affairs [now Committee on Homeland Security and Governmental Affairs] of the Senate and the Committee on Government Reform [now Committee on Oversight and Accountability] of the House of Representatives on progress toward integrating Federal information systems across agencies.

''(2) CONTENTS.—The report under this section shall—

''(A) address the integration of data elements used in the electronic collection of information within databases established under Federal statute without reducing the quality, accessibility, scope, or utility of the information contained in each database;

''(B) address the feasibility of developing, or enabling the development of, software, including Internet-based tools, for use by reporting persons in assembling, documenting, and validating the accuracy of information electronically submitted to agencies under nonvoluntary, statutory, and regulatory requirements;

''(C) address the feasibility of developing a distributed information system involving, on a voluntary basis, at least 2 agencies, that—

''(i) provides consistent, dependable, and timely public access to the information holdings of 1 or more agencies, or some portion of such holdings, without requiring public users to know which agency holds the information; and

''(ii) allows the integration of public information held by the participating agencies;

''(D) address the feasibility of incorporating other elements related to the purposes of this section at the discretion of the Director; and

''(E) make any recommendations that the Director deems appropriate on the use of integrated reporting and information systems, to reduce the burden on reporting and strengthen public access to databases within and across agencies.

''(d) PILOT PROJECTS TO ENCOURAGE INTEGRATED COLLECTION AND MANAGEMENT OF DATA AND INTEROPERABILITY OF FEDERAL INFORMATION SYSTEMS.—

''(1) IN GENERAL.—In order to provide input to the study under subsection (c), the Director shall designate, in consultation with agencies, a series of no more than 5 pilot projects that integrate data elements. The Director shall consult with agencies, the regulated community, public interest organizations, and the public on the implementation of the pilot projects.

''(2) GOALS OF PILOT PROJECTS.—

''(A) IN GENERAL.—Each goal described under subparagraph (B) shall be addressed by at least 1 pilot project each.

''(B) GOALS.—The goals under this paragraph are to—

''(i) reduce information collection burdens by eliminating duplicative data elements within 2 or more reporting requirements;

''(ii) create interoperability between or among public databases managed by 2 or more agencies using technologies and techniques that facilitate public access; and

''(iii) develop, or enable the development of, software to reduce errors in electronically submitted information.

''(3) INPUT.—Each pilot project shall seek input from users on the utility of the pilot project and areas for improvement. To the extent practicable, the Director shall consult with relevant agencies and State, tribal, and local governments in carrying out the report and pilot projects under this section.

''(e) PROTECTIONS.—The activities authorized under this section shall afford protections for—

''(1) confidential business information consistent with section 552(b)(4) of title 5, United States Code, and other relevant law;

''(2) personal privacy information under sections 552(b)(6) and (7)(C) and 552a of title 5, United States Code, and other relevant law;

''(3) other information consistent with section 552(b)(3) of title 5, United States Code, and other relevant law; and

''(4) confidential statistical information collected under a confidentiality pledge, solely for statistical purposes, consistent with the Office of Management and Budget's Federal Statistical Confidentiality Order, and other relevant law.

''SEC. 213. COMMUNITY TECHNOLOGY CENTERS.

''(a) PURPOSES.—The purposes of this section are to—

''(1) study and enhance the effectiveness of community technology centers, public libraries, and other institutions that provide computer and Internet access to the public; and

''(2) promote awareness of the availability of online government information and services, to users of community technology centers, public libraries, and other public facilities that provide access to computer technology and Internet access to the public.

''(b) STUDY AND REPORT.—Not later than 2 years after the effective date of this title [see Effective Date note

set out under section 3601 of this title], the Administrator shall—

''(1) ensure that a study is conducted to evaluate the best practices of community technology centers that have received Federal funds; and

''(2) submit a report on the study to—

''(A) the Committee on Governmental Affairs [now Committee on Homeland Security and Governmental Affairs] of the Senate;

''(B) the Committee on Health, Education, Labor, and Pensions of the Senate;

''(C) the Committee on Government Reform [now Committee on Oversight and Accountability] of the House of Representatives; and

''(D) the Committee on Education and the Workforce of the House of Representatives.

''(c) CONTENTS.—The report under subsection (b) may consider—

''(1) an evaluation of the best practices being used by successful community technology centers;

''(2) a strategy for—

''(A) continuing the evaluation of best practices used by community technology centers; and

''(B) establishing a network to share information and resources as community technology centers evolve;

''(3) the identification of methods to expand the use of best practices to assist community technology centers, public libraries, and other institutions that provide computer and Internet access to the public;

''(4) a database of all community technology centers that have received Federal funds, including—

''(A) each center's name, location, services provided, director, other points of contact, number of individuals served; and

''(B) other relevant information;

''(5) an analysis of whether community technology centers have been deployed effectively in urban and rural areas throughout the Nation; and

''(6) recommendations of how to—

''(A) enhance the development of community technology centers; and

''(B) establish a network to share information and resources.

''(d) COOPERATION.—All agencies that fund community technology centers shall provide to the Administrator any information and assistance necessary for the completion of the study and the report under this section.

''(e) ASSISTANCE.—

''(1) IN GENERAL.—The Administrator, in consultation with the Secretary of Education, shall work with other relevant Federal agencies, and other interested persons in the private and nonprofit sectors to—

''(A) assist in the implementation of recommendations; and

''(B) identify other ways to assist community technology centers, public libraries, and other institutions that provide computer and Internet access to the public.

''(2) TYPES OF ASSISTANCE.—Assistance under this subsection may include—

''(A) contribution of funds;

''(B) donations of equipment, and training in the use and maintenance of the equipment; and

''(C) the provision of basic instruction or training material in computer skills and Internet usage.

''(f) ONLINE TUTORIAL.—

''(1) IN GENERAL.—The Administrator, in consultation with the Secretary of Education, the Director of the Institute of Museum and Library Services, other relevant agencies, and the public, shall develop an online tutorial that—

''(A) explains how to access Government information and services on the Internet; and

''(B) provides a guide to available online resources.

''(2) DISTRIBUTION.—The Administrator, with assistance from the Secretary of Education, shall distribute information on the tutorial to community technology centers, public libraries, and other institutions that afford Internet access to the public.

''(g) PROMOTION OF COMMUNITY TECHNOLOGY CENTERS.—The Administrator, with assistance from the Department of Education and in consultation with other agencies and organizations, shall promote the availability of community technology centers to raise awareness within each community where such a center is located.

''(h) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated for the study of best practices at community technology centers, for the development and dissemination of the online tutorial, and for the promotion of community technology centers under this section—

''(1) $2,000,000 in fiscal year 2003;

''(2) $2,000,000 in fiscal year 2004; and

''(3) such sums as are necessary in fiscal years 2005 through 2007.

''SEC. 214. ENHANCING CRISIS MANAGEMENT THROUGH ADVANCED INFORMATION TECHNOLOGY.

''(a) PURPOSE.—The purpose of this section is to improve how information technology is used in coordinating and facilitating information on disaster preparedness, response, and recovery, while ensuring the availability of such information across multiple access channels.

''(b) IN GENERAL.—

''(1) STUDY ON ENHANCEMENT OF CRISIS RESPONSE.—Not later than 90 days after the date of enactment of this Act [Dec. 17, 2002], the Administrator, in consultation with the Federal Emergency Management Agency, shall ensure that a study is conducted on using information technology to enhance crisis preparedness, response, and consequence management of natural and manmade disasters.

''(2) CONTENTS.—The study under this subsection shall address—

''(A) a research and implementation strategy for effective use of information technology in crisis response and consequence management, including the more effective use of technologies, management of information technology research initiatives, and incorporation of research advances into the information and communications systems of—

''(i) the Federal Emergency Management Agency; and

''(ii) other Federal, State, and local agencies responsible for crisis preparedness, response, and consequence management; and

''(B) opportunities for research and development on enhanced technologies into areas of potential improvement as determined during the course of the study.

''(3) REPORT.—Not later than 2 years after the date on which a contract is entered into under paragraph (1), the Administrator shall submit a report on the study, including findings and recommendations to—

''(A) the Committee on Governmental Affairs [now Committee on Homeland Security and Governmental Affairs] of the Senate; and

''(B) the Committee on Government Reform [now Committee on Oversight and Accountability] of the House of Representatives.

''(4) INTERAGENCY COOPERATION.—Other Federal departments and agencies with responsibility for disaster relief and emergency assistance shall fully cooperate with the Administrator in carrying out this section.

''(5) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated for research under this subsection, such sums as are necessary for fiscal year 2003.

''(c) PILOT PROJECTS.—Based on the results of the research conducted under subsection (b), the Administrator, in consultation with the Federal Emergency Management Agency, shall initiate pilot projects or report to Congress on other activities that further the

goal of maximizing the utility of information technology in disaster management. The Administrator shall cooperate with other relevant agencies, and, if appropriate, State, local, and tribal governments, in initiating such pilot projects.

''SEC. 215. DISPARITIES IN ACCESS TO THE INTERNET.

''(a) STUDY AND REPORT.—

''(1) STUDY.—Not later than 90 days after the date of enactment of this Act [Dec. 17, 2002], the Administrator of General Services shall request that the National Academy of Sciences, acting through the National Research Council, enter into a contract to conduct a study on disparities in Internet access for online Government services.

''(2) REPORT.—Not later than 2 years after the date of enactment of this Act, the Administrator of General Services shall submit to the Committee on Governmental Affairs [now Committee on Homeland Security and Governmental Affairs] of the Senate and the Committee on Government Reform [now Committee on Oversight and Accountability] of the House of Representatives a final report of the study under this section, which shall set forth the findings, conclusions, and recommendations of the National Research Council.

''(b) CONTENTS.—The report under subsection (a) shall include a study of—

''(1) how disparities in Internet access influence the effectiveness of online Government services, including a review of—

''(A) the nature of disparities in Internet access;

''(B) the affordability of Internet service;

''(C) the incidence of disparities among different groups within the population; and

''(D) changes in the nature of personal and public Internet access that may alleviate or aggravate effective access to online Government services;

''(2) how the increase in online Government services is influencing the disparities in Internet access and how technology development or diffusion trends may offset such adverse influences; and

''(3) related societal effects arising from the interplay of disparities in Internet access and the increase in online Government services.

''(c) RECOMMENDATIONS.—The report shall include recommendations on actions to ensure that online Government initiatives shall not have the unintended result of increasing any deficiency in public access to Government services.

''(d) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated $950,000 in fiscal year 2003 to carry out this section.

''SEC. 216. COMMON PROTOCOLS FOR GEOGRAPHIC INFORMATION SYSTEMS.

''(a) PURPOSES.—The purposes of this section are to—

''(1) reduce redundant data collection and information; and

''(2) promote collaboration and use of standards for government geographic information.

''(b) DEFINITION.—In this section, the term 'geographic information' means information systems that involve locational data, such as maps or other geospatial information resources.

''(c) IN GENERAL.—

''(1) COMMON PROTOCOLS.—The Administrator, in consultation with the Secretary of the Interior, working with the Director and through an interagency group, and working with private sector experts, State, local, and tribal governments, commercial and international standards groups, and other interested parties, shall facilitate the development of common protocols for the development, acquisition, maintenance, distribution, and application of geographic information. If practicable, the Administrator shall incorporate intergovernmental and public private geographic information partnerships into efforts under this subsection.

''(2) INTERAGENCY GROUP.—The interagency group referred to under paragraph (1) shall include representatives of the National Institute of Standards and Technology and other agencies.

''(d) DIRECTOR.—The Director shall oversee—

''(1) the interagency initiative to develop common protocols;

''(2) the coordination with State, local, and tribal governments, public private partnerships, and other interested persons on effective and efficient ways to align geographic information and develop common protocols; and

''(3) the adoption of common standards relating to the protocols.

''(e) COMMON PROTOCOLS.—The common protocols shall be designed to—

''(1) maximize the degree to which unclassified geographic information from various sources can be made electronically compatible and accessible; and

''(2) promote the development of interoperable geographic information systems technologies that shall—

''(A) allow widespread, low-cost use and sharing of geographic data by Federal agencies, State, local, and tribal governments, and the public; and

''(B) enable the enhancement of services using geographic data.

''(f) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated such sums as are necessary to carry out this section, for each of the fiscal years 2003 through 2007.''

INFORMATION SECURITY RESPONSIBILITIES OF CERTAIN AGENCIES

Pub. L. 107–347, title III, §301(c)(1)(A), Dec. 17, 2002, 116 Stat. 2955, provided that: ''Nothing in this Act [see Tables for classification] (including any amendment made by this Act) shall supersede any authority of the Secretary of Defense, the Director of Central Intelligence, or other agency head, as authorized by law and as directed by the President, with regard to the operation, control, or management of national security systems, as defined by [former] section 3542(b)(2) of title 44, United States Code [see now 44 U.S.C. 3552(b)(6)].''

[Reference to the Director of Central Intelligence or the Director of the Central Intelligence Agency in the Director's capacity as the head of the intelligence community deemed to be a reference to the Director of National Intelligence. Reference to the Director of Central Intelligence or the Director of the Central Intelligence Agency in the Director's capacity as the head of the Central Intelligence Agency deemed to be a reference to the Director of the Central Intelligence Agency. See section 1081(a), (b) of Pub. L. 108–458, set out as a note under section 3001 of Title 50, War and National Defense.]

ATOMIC ENERGY ACT OF 1954

Pub. L. 107–347, title III, §301(c)(2), Dec. 17, 2002, 116 Stat. 2955, provided that: ''Nothing in this Act [see Tables for classification] shall supersede any requirement made by or under the Atomic Energy Act of 1954 (42 U.S.C. 2011 et seq.). Restricted data or formerly restricted data shall be handled, protected, classified, downgraded, and declassified in conformity with the Atomic Energy Act of 1954 (42 U.S.C. 2011 et seq.).''

CONFIDENTIAL INFORMATION PROTECTION AND STATISTICAL EFFICIENCY

Pub. L. 107–347, title V, Dec. 17, 2002, 116 Stat. 2962, which related to confidential information protection and statistical efficiency, was repealed by Pub. L. 115–435, title III, §302(c)(1), title IV, §403, Jan. 14, 2019, 132 Stat. 5552, 5557, effective 180 days after Jan. 14, 2019, and restated as parts A to C of subchapter III of this chapter. See Transitional and Savings Provisions note set out under section 3561 of this title.

WAIVER OF PAPERWORK REDUCTION

Pub. L. 101–508, title IV, §4711(f), Nov. 5, 1990, 104 Stat. 1388–187, provided that: ''Chapter 35 of title 44, United

States Code, and Executive Order 12291 [formerly set out as a note under section 601 of Title 5, Government Organization and Employees] shall not apply to information and regulations required for purposes of carrying out this Act [see Tables for classification] and implementing the amendments made by this Act.''

Executive Documents

EX. ORD. NO. 13556. CONTROLLED UNCLASSIFIED INFORMATION

Ex. Ord. No. 13556, Nov. 4, 2010, 75 F.R. 68675, provided:

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

SECTION 1. *Purpose*. This order establishes an open and uniform program for managing information that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government-wide policies, excluding information that is classified under Executive Order 13526 of December 29, 2009, or the Atomic Energy Act, as amended.

At present, executive departments and agencies (agencies) employ ad hoc, agency-specific policies, procedures, and markings to safeguard and control this information, such as information that involves privacy, security, proprietary business interests, and law enforcement investigations. This inefficient, confusing patchwork has resulted in inconsistent marking and safeguarding of documents, led to unclear or unnecessarily restrictive dissemination policies, and created impediments to authorized information sharing. The fact that these agency-specific policies are often hidden from public view has only aggravated these issues.

To address these problems, this order establishes a program for managing this information, hereinafter described as Controlled Unclassified Information, that emphasizes the openness and uniformity of Government-wide practice.

SEC. 2. *Controlled Unclassified Information (CUI).*

(a) The CUI categories and subcategories shall serve as exclusive designations for identifying unclassified information throughout the executive branch that requires safeguarding or dissemination controls, pursuant to and consistent with applicable law, regulations, and Government-wide policies.

(b) The mere fact that information is designated as CUI shall not have a bearing on determinations pursuant to any law requiring the disclosure of information or permitting disclosure as a matter of discretion, including disclosures to the legislative or judicial branches.

(c) The National Archives and Records Administration shall serve as the Executive Agent to implement this order and oversee agency actions to ensure compliance with this order.

SEC. 3. *Review of Current Designations.*

(a) Each agency head shall, within 180 days of the date of this order:

(1) review all categories, subcategories, and markings used by the agency to designate unclassified information for safeguarding or dissemination controls; and

(2) submit to the Executive Agent a catalogue of proposed categories and subcategories of CUI, and proposed associated markings for information designated as CUI under section 2(a) of this order. This submission shall provide definitions for each proposed category and subcategory and identify the basis in law, regulation, or Government-wide policy for safeguarding or dissemination controls.

(b) If there is significant doubt about whether information should be designated as CUI, it shall not be so designated.

SEC. 4. *Development of CUI Categories and Policies.*

(a) On the basis of the submissions under section 3 of this order or future proposals, and in consultation with affected agencies, the Executive Agent shall, in a timely manner, approve categories and subcategories of CUI and associated markings to be applied uniformly throughout the executive branch and to become effective upon publication in the registry established under subsection (d) of this section. No unclassified information meeting the requirements of section 2(a) of this order shall be disapproved for inclusion as CUI, but the Executive Agent may resolve conflicts among categories and subcategories of CUI to achieve uniformity and may determine the markings to be used.

(b) The Executive Agent, in consultation with affected agencies, shall develop and issue such directives as are necessary to implement this order. Such directives shall be made available to the public and shall provide policies and procedures concerning marking, safeguarding, dissemination, and decontrol of CUI that, to the extent practicable and permitted by law, regulation, and Government-wide policies, shall remain consistent across categories and subcategories of CUI and throughout the executive branch. In developing such directives, appropriate consideration should be given to the report of the interagency Task Force on Controlled Unclassified Information published in August 2009. The Executive Agent shall issue initial directives for the implementation of this order within 180 days of the date of this order.

(c) The Executive Agent shall convene and chair interagency meetings to discuss matters pertaining to the program established by this order.

(d) Within 1 year of the date of this order, the Executive Agent shall establish and maintain a public CUI registry reflecting authorized CUI categories and subcategories, associated markings, and applicable safeguarding, dissemination, and decontrol procedures.

(e) If the Executive Agent and an agency cannot reach agreement on an issue related to the implementation of this order, that issue may be appealed to the President through the Director of the Office of Management and Budget.

(f) In performing its functions under this order, the Executive Agent, in accordance with applicable law, shall consult with representatives of the public and State, local, tribal, and private sector partners on matters related to approving categories and subcategories of CUI and developing implementing directives issued by the Executive Agent pursuant to this order.

SEC. 5. *Implementation.*

(a) Within 180 days of the issuance of initial policies and procedures by the Executive Agent in accordance with section 4(b) of this order, each agency that originates or handles CUI shall provide the Executive Agent with a proposed plan for compliance with the requirements of this order, including the establishment of interim target dates.

(b) After a review of agency plans, and in consultation with affected agencies and the Office of Management and Budget, the Executive Agent shall establish deadlines for phased implementation by agencies.

(c) In each of the first 5 years following the date of this order and biennially thereafter, the Executive Agent shall publish a report on the status of agency implementation of this order.

SEC. 6. *General Provisions.*

(a) This order shall be implemented in a manner consistent with:

(1) applicable law, including protections of confidentiality and privacy rights;

(2) the statutory authority of the heads of agencies, including authorities related to the protection of information provided by the private sector to the Federal Government; and

(3) applicable Government-wide standards and guidelines issued by the National Institute of Standards and Technology, and applicable policies established by the Office of Management and Budget.

(b) The Director of National Intelligence (Director), with respect to the Intelligence Community and after consultation with the heads of affected agencies, may issue such policy directives and guidelines as the Director deems necessary to implement this order with respect to intelligence and intelligence-related information. Procedures or other guidance issued by Intel-

ligence Community element heads shall be in accordance with such policy directives or guidelines issued by the Director. Any such policy directives or guidelines issued by the Director shall be in accordance with this order and directives issued by the Executive Agent.

(c) This order shall not be construed to impair or otherwise affect the functions of the Director of the Office of Management and Budget relating to budgetary, administrative, and legislative proposals.

(d) This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

(e) This order shall be implemented subject to the availability of appropriations.

(f) The Attorney General, upon request by the head of an agency or the Executive Agent, shall render an interpretation of this order with respect to any question arising in the course of its administration.

(g) The Presidential Memorandum of May 7, 2008, entitled ''Designation and Sharing of Controlled Unclassified Information (CUI)'' is hereby rescinded.

BARACK OBAMA.

MAKING IT EASIER FOR AMERICA'S SMALL BUSINESSES AND AMERICA'S EXPORTERS TO ACCESS GOVERNMENT SERVICES TO HELP THEM GROW AND HIRE

Memorandum of President of the United States, Oct. 28, 2011, 76 F.R. 68049, provided:

Memorandum for the Heads of Executive Departments and Agencies

As I outlined in my State of the Union address to the Congress on January 25, 2011, winning the future in the global economy will require a Government that wisely allocates its scarce resources to maximize efficiency and effectiveness so that it can best support American competitiveness, innovation, and job growth. If we are to thrive in the global economy, and make America the best place on Earth to do business, we need to equip our Government with the tools necessary to support innovation and job growth in the 21st century.

Accordingly, we must make it easier for businesses to access the full range of Government programs and services without having to waste effort navigating their way through the Federal bureaucracy. At the same time, we must further streamline and coordinate Federal programs to reduce costs and provide customer-oriented service.

Businesses looking for assistance from the Federal Government should feel like they are interacting with one entity, rather than a number of separate, albeit linked, components. This means adopting a ''No Wrong Door'' policy that uses technology to quickly connect businesses to the services and information relevant to them, regardless of which agency's website, call center, or office they go to for help.

In addition, a business's interactions with the Federal Government should be individualized and efficient. If the private sector can allow consumers to customize interactions so that they receive only the information they want, in the form they want it, so can the Federal Government.

Today, I am directing a first wave of changes focused on both small businesses and businesses of all sizes that want to begin or increase exporting (exporters), because those businesses help drive economic growth and have the most to gain from Federal assistance. We plan to use the resulting improvements as a model for future reforms so that, in time, all businesses and all citizens receive the highest level of customer service when they interact with the Federal Government.

Accordingly, I direct the following:

(1) All executive departments and agencies (agencies) shall work with a Steering Committee co-chaired by the Federal Chief Information Officer, Assistant to the President and Chief Technology Officer, and Chief Performance Officer (the Co-Chairs) to carry out the directives in this memorandum within 90 days of the date of this memorandum, unless a provision of this memorandum expressly states otherwise. The Steering Committee shall include senior policy and technical representatives, appointed by the heads of their respective agencies, from the Departments of State, Defense, Agriculture, Commerce, and Veterans Affairs, the Small Business Administration (SBA), the General Services Administration (GSA), the Export-Import Bank, and other agencies designated by the Co-Chairs. The Co-Chairs and representatives from the Department of Commerce and SBA shall serve as the Executive Committee of the Steering Committee, which shall coordinate the strategy, design, development, launch, and operation of BusinessUSA, a common, open, online platform and web service with dedicated resources that will, as a first step, disseminate core information regarding the Federal Government's programs and services relevant to small businesses and exporters.

(2) Agencies shall work with the Steering Committee to develop and launch an introductory version of BusinessUSA. BusinessUSA shall be designed, tested, and built with the active feedback of U.S. businesses and relevant online communities. To the extent appropriate, practicable, and permitted by law, the BusinessUSA platform shall integrate related State and local government services as well as those of private sector partners.

(3) Agencies shall make information regarding their small business and export programs and services accessible through BusinessUSA. To accomplish this in a uniform fashion, the Steering Committee shall develop a common set of standards for content available through BusinessUSA, which shall identify the types of programs and services to be included initially on BusinessUSA and a structure for organizing and presenting such information. These standards shall be used by all agencies in the creation, presentation, and delivery of information regarding their programs and services, to the extent practicable and permitted by law.

(4) Agencies shall also work with the Steering Committee to develop new content for BusinessUSA that synthesizes information available across agencies to better serve small businesses and exporters. Among other things, agencies shall work together to aggregate on the BusinessUSA platform statistical, demographic, and other raw Government datasets of particular interest to small businesses and exporters, making Government data more easily accessible and spurring innovative uses of the data through business-oriented web or mobile applications.

(5) Agencies shall integrate BusinessUSA, including ready access to the BusinessUSA website, into their current websites, call centers, and field offices to ensure that small businesses and exporters have access to the wide range of Government programs and services at each entry point into the Federal Government. During the year following the date of this memorandum, agencies shall work with GSA and the Office of Management and Budget to enhance the centralized call center for responding to public questions about Federal programs and services (1–800–FED–INFO) to add expertise with Government programs and services for small businesses and exporters.

(6) (a) Nothing in this memorandum shall be construed to impair or otherwise affect:

(i) authority granted by law or Executive Order to an agency, or the head thereof; or

(ii) functions of the Director of the Office of Management and Budget relating to budgetary, administrative, or legislative proposals.

(b) BusinessUSA shall be operated by a single hosting agency under the Executive Committee's coordination. To the extent permitted by law, agencies shall reimburse the hosting agency for the cost of establishing, maintaining, and operating BusinessUSA.

(c) This memorandum shall be implemented consistent with applicable law and subject to the availability of appropriations.

(d) This memorandum is not intended to, and does not, create any right or benefit, substantive or proce-

dural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

(7) The Director of the Office of Management and Budget is authorized and directed to publish this memorandum in the Federal Register.

BARACK OBAMA.

§ 3502. Definitions

As used in this subchapter—

(1) the term ''agency'' means any executive department, military department, Government corporation, Government controlled corporation, or other establishment in the executive branch of the Government (including the Executive Office of the President), or any independent regulatory agency, but does not include—

(A) the Government Accountability Office;

(B) Federal Election Commission;

(C) the governments of the District of Columbia and of the territories and possessions of the United States, and their various subdivisions; or

(D) Government-owned contractor-operated facilities, including laboratories engaged in national defense research and production activities;

(2) the term ''burden'' means time, effort, or financial resources expended by persons to generate, maintain, or provide information to or for a Federal agency, including the resources expended for—

(A) reviewing instructions;

(B) acquiring, installing, and utilizing technology and systems;

(C) adjusting the existing ways to comply with any previously applicable instructions and requirements;

(D) searching data sources;

(E) completing and reviewing the collection of information; and

(F) transmitting, or otherwise disclosing the information;

(3) the term ''collection of information''—

(A) means the obtaining, causing to be obtained, soliciting, or requiring the disclosure to third parties or the public, of facts or opinions by or for an agency, regardless of form or format, calling for either—

(i) answers to identical questions posed to, or identical reporting or recordkeeping requirements imposed on, ten or more persons, other than agencies, instrumentalities, or employees of the United States; or

(ii) answers to questions posed to agencies, instrumentalities, or employees of the United States which are to be used for general statistical purposes; and

(B) shall not include a collection of information described under section 3518(c)(1);

(4) the term ''Director'' means the Director of the Office of Management and Budget;

(5) the term ''independent regulatory agency'' means the Board of Governors of the Federal Reserve System, the Commodity Futures Trading Commission, the Consumer Product Safety Commission, the Federal Communications Commission, the Federal Deposit Insurance Corporation, the Federal Energy Regulatory Commission, the Federal Housing Finance Agency, the Federal Maritime Commission, the Federal Trade Commission, the Interstate Commerce Commission, the Mine Enforcement Safety and Health Review Commission, the National Labor Relations Board, the Nuclear Regulatory Commission, the Occupational Safety and Health Review Commission, the Postal Regulatory Commission, the Securities and Exchange Commission, the Bureau of Consumer Financial Protection, the Office of Financial Research, Office of the Comptroller of the Currency, and any other similar agency designated by statute as a Federal independent regulatory agency or commission;

(6) the term ''information resources'' means information and related resources, such as personnel, equipment, funds, and information technology;

(7) the term ''information resources management'' means the process of managing information resources to accomplish agency missions and to improve agency performance, including through the reduction of information collection burdens on the public;

(8) the term ''information system'' means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information;

(9) the term ''information technology'' has the meaning given that term in section 11101 of title 40 but does not include national security systems as defined in section 11103 of title 40;

(10) the term ''person'' means an individual, partnership, association, corporation, business trust, or legal representative, an organized group of individuals, a State, territorial, tribal, or local government or branch thereof, or a political subdivision of a State, territory, tribal, or local government or a branch of a political subdivision;

(11) the term ''practical utility'' means the ability of an agency to use information, particularly the capability to process such information in a timely and useful fashion;

(12) the term ''public information'' means any information, regardless of form or format, that an agency discloses, disseminates, or makes available to the public;

(13) the term ''recordkeeping requirement'' means a requirement imposed by or for an agency on persons to maintain specified records, including a requirement to—

(A) retain such records;

(B) notify third parties, the Federal Government, or the public of the existence of such records;

(C) disclose such records to third parties, the Federal Government, or the public; or

(D) report to third parties, the Federal Government, or the public regarding such records;

(14) the term ''penalty'' includes the imposition by an agency or court of a fine or other punishment; a judgment for monetary damages or equitable relief; or the revocation, suspension, reduction, or denial of a license, privilege, right, grant, or benefit;

(15) the term ''comprehensive data inventory'' means the inventory created under section 3511(a), but does not include any underlying data asset listed on the inventory;

(16) the term ''data'' means recorded information, regardless of form or the media on which the data is recorded;

(17) the term ''data asset'' means a collection of data elements or data sets that may be grouped together;

(18) the term ''machine-readable'', when used with respect to data, means data in a format that can be easily processed by a computer without human intervention while ensuring no semantic meaning is lost;

(19) the term ''metadata'' means structural or descriptive information about data such as content, format, source, rights, accuracy, provenance, frequency, periodicity, granularity, publisher or responsible party, contact information, method of collection, and other descriptions;

(20) the term ''open Government data asset'' means a public data asset that is—

(A) machine-readable;

(B) available (or could be made available) in an open format;

(C) not encumbered by restrictions, other than intellectual property rights, including under titles 17 and 35, that would impede the use or reuse of such asset; and

(D) based on an underlying open standard that is maintained by a standards organization;

(21) the term ''open license'' means a legal guarantee that a data asset is made available—

(A) at no cost to the public; and

(B) with no restrictions on copying, publishing, distributing, transmitting, citing, or adapting such asset;

(22) the term ''public data asset'' means a data asset, or part thereof, maintained by the Federal Government that has been, or may be, released to the public, including any data asset, or part thereof, subject to disclosure under section 552 of title 5; and

(23) the term ''statistical laws'' means subchapter III of this chapter and other laws pertaining to the protection of information collected for statistical purposes as designated by the Director.

(Added Pub. L. 104–13, §2, May 22, 1995, 109 Stat. 164; amended Pub. L. 104–106, div. E, title LVI, §5605(a), Feb. 10, 1996, 110 Stat. 700; Pub. L. 105–85, div. A, title X, §1073(h)(5)(A), Nov. 18, 1997, 111 Stat. 1907; Pub. L. 106–398, §1 [[div. A], title X, §1064(b)], Oct. 30, 2000, 114 Stat. 1654, 1654A–275; Pub. L. 107–217, §3(*l*)(4), Aug. 21, 2002, 116 Stat. 1301; Pub. L. 108–271, §8(b), July 7, 2004, 118 Stat. 814; Pub. L. 109–435, title VI, §604(e), Dec. 20, 2006, 120 Stat. 3242; Pub. L. 110–289, div. A, title II, §1216(e), July 30, 2008, 122 Stat. 2792; Pub. L. 111–203, title III, §315, title X, §1100D(a), July 21, 2010, 124 Stat. 1524, 2111; Pub. L. 115–435, title II, §202(a), Jan. 14, 2019, 132 Stat. 5534.)

Editorial Notes

Prior Provisions

A prior section 3502, added Pub. L. 96–511, §2(a), Dec. 11, 1980, 94 Stat. 2813; amended Pub. L. 98–443, §9(h), Oct. 4, 1984, 98 Stat. 1708; Pub. L. 99–500, §101(m) [title VIII, §812], Oct. 18, 1986, 100 Stat. 1783–308, 1783–335, and Pub. L. 99–591, §101(m) [title VIII, §812], Oct. 30, 1986, 100 Stat. 3341–308, 3341–335; Pub. L. 101–73, title VII, §744(e), Aug. 9, 1989, 103 Stat. 438, defined terms used in this chapter prior to the general amendment of this chapter by Pub. L. 104–13.

Another prior section 3502, Pub. L. 90–620, Oct. 22, 1968, 82 Stat. 1302; Pub. L. 93–153, title IV, §409(a), Nov. 16, 1973, 87 Stat. 593, defined ''Federal agency'', ''person'', and ''information'', prior to the general amendment of this chapter by Pub. L. 96–511.

Amendments

2019—Pars. (15) to (23). Pub. L. 115–435 added pars. (15) to (23).

2010—Par. (5). Pub. L. 111–203, §1100D(a), which directed amendment of section 2(5) of the Paperwork Reduction Act (44 U.S.C. 3502(5)) by inserting ''the Bureau of Consumer Financial Protection, the Office of Financial Research,'' after ''the Securities and Exchange Commission,'', was executed to this section to reflect the probable intent of Congress.

Pub. L. 111–203, §315, inserted ''Office of the Comptroller of the Currency,'' after ''the Securities and Exchange Commission,''.

2008—Par. (5). Pub. L. 110–289 substituted ''Federal Housing Finance Agency'' for ''Federal Housing Finance Board''.

2006—Par. (5). Pub. L. 109–435 substituted ''Postal Regulatory Commission'' for ''Postal Rate Commission''.

2004—Par. (1)(A). Pub. L. 108–271 substituted ''Government Accountability Office'' for ''General Accounting Office''.

2002—Par. (9). Pub. L. 107–217 substituted ''section 11101 of title 40'' for ''section 5002 of the Clinger-Cohen Act of 1996 (40 U.S.C. 1401)'' and ''section 11103 of title 40'' for ''section 5142 of that Act (40 U.S.C. 1452)''.

2000—Pub. L. 106–398 substituted ''subchapter'' for ''chapter'' in introductory provisions.

1997—Par. (9). Pub. L. 105–85 substituted ''the Clinger-Cohen Act of 1996 (40 U.S.C. 1401)'' for ''the Information Technology Management Reform Act of 1996'' and inserted ''(40 U.S.C. 1452)'' after ''that Act''.

1996—Par. (9). Pub. L. 104–106 added par. (9) and struck out former par. (9) which read as follows: ''the term 'information technology' has the same meaning as the term 'automatic data processing equipment' as defined by section 111(a)(2) and (3)(C)(i) through (v) of the Federal Property and Administrative Services Act of 1949 (40 U.S.C. 759(a)(2) and (3)(C)(i) through (v));''.

Statutory Notes and Related Subsidiaries

Effective Date of 2019 Amendment

Amendment by Pub. L. 115–435 effective 180 days after Jan. 14, 2019, see section 403 of Pub. L. 115–435, set out as a note under section 306 of Title 5, Government Organization and Employees.

Effective Date of 2010 Amendment

Amendment by section 315 of Pub. L. 111–203 effective 1 day after July 21, 2010, except as otherwise provided, see section 4 of Pub. L. 111–203, set out as an Effective Date note under section 5301 of Title 12, Banks and Banking.

Amendment by section 1100D(a) of Pub. L. 111–203 effective on the designated transfer date, see section 1100H of Pub. L. 111–203, set out as a note under section 552a of Title 5, Government Organization and Employees.

Effective Date of 2000 Amendment

Amendment by Pub. L. 106–398 effective 30 days after Oct. 30, 2000, see section 1 [[div. A], title X, §1065] of Pub. L. 106–398, Oct. 30, 2000, 114 Stat. 1654, formerly set out as an Effective Date note under former section 3531 of this title.

EFFECTIVE DATE OF 1996 AMENDMENT

Amendment by Pub. L. 104–106 effective 180 days after Feb. 10, 1996, see section 5701 of Pub. L. 104–106, Feb. 10, 1996, 110 Stat. 702.

EFFECTIVE DATE

Section effective Oct. 1, 1995, except as otherwise provided, see section 4(a) of Pub. L. 104–13, set out as a note under section 3501 of this title.

ABOLITION OF INTERSTATE COMMERCE COMMISSION AND TRANSFER OF FUNCTIONS

Interstate Commerce Commission abolished and functions of Commission transferred, except as otherwise provided in Pub. L. 104–88, to Surface Transportation Board effective Jan. 1, 1996, by section 1302 of Title 49, Transportation, and section 101 of Pub. L. 104–88, set out as a note under section 1301 of Title 49. References to Interstate Commerce Commission deemed to refer to Surface Transportation Board, a member or employee of the Board, or Secretary of Transportation, as appropriate, see section 205 of Pub. L. 104–88, set out as a note under section 1301 of Title 49.

§ 3503. Office of Information and Regulatory Affairs

(a) There is established in the Office of Management and Budget an office to be known as the Office of Information and Regulatory Affairs.

(b) There shall be at the head of the Office an Administrator who shall be appointed by the President, by and with the advice and consent of the Senate. The Director shall delegate to the Administrator the authority to administer all functions under this subchapter, except that any such delegation shall not relieve the Director of responsibility for the administration of such functions. The Administrator shall serve as principal adviser to the Director on Federal information resources management policy.

(Added Pub. L. 104–13, § 2, May 22, 1995, 109 Stat. 166; amended Pub. L. 106–398, § 1 [[div. A], title X, § 1064(b)], Oct. 30, 2000, 114 Stat. 1654, 1654A–275.)

Editorial Notes

PRIOR PROVISIONS

A prior section 3503, added Pub. L. 96–511, § 2(a), Dec. 11, 1980, 94 Stat. 2814; amended Pub. L. 99–500, § 101(m) [title VIII, § 813(a)], Oct. 18, 1986, 100 Stat. 1783–308, 1783–336, and Pub. L. 99–591, § 101(m) [title VIII, § 813(a)], Oct. 30, 1986, 100 Stat. 3341–308, 3341–336, related to the establishment of the Office of Information and Regulatory Affairs prior to the general amendment of this chapter by Pub. L. 104–13.

Another prior section 3503, Pub. L. 90–620, Oct. 22, 1968, 82 Stat. 1303, prescribed duties of Director of Bureau of the Budget, prior to the general amendment of this chapter by Pub. L. 96–511. See section 3504 of this title.

AMENDMENTS

2000—Subsec. (b). Pub. L. 106–398 substituted ''subchapter'' for ''chapter''.

Statutory Notes and Related Subsidiaries

EFFECTIVE DATE OF 2000 AMENDMENT

Amendment by Pub. L. 106–398 effective 30 days after Oct. 30, 2000, see section 1 [[div. A], title X, § 1065] of Pub. L. 106–398, Oct. 30, 2000, 114 Stat. 1654, formerly set out as an Effective Date note under former section 3531 of this title.

EFFECTIVE DATE

Section effective Oct. 1, 1995, except as otherwise provided, see section 4(a) of Pub. L. 104–13, set out as a note under section 3501 of this title.

DELEGATION OF OTHER FUNCTIONS TO ADMINISTRATOR

Pub. L. 96–511, § 3, Dec. 11, 1980, 94 Stat. 2825, as amended by Pub. L. 97–258, § 5(b), Sept. 13, 1982, 96 Stat. 1083; Pub. L. 99–500, § 101(m) [title VIII, § 821(b)(3)], Oct. 18, 1986, 100 Stat. 1783–308, 1783–342, and Pub. L. 99–591, § 101(m) [title VIII, § 821(b)(3)], Oct. 30, 1986, 100 Stat. 3341–308, 3341–342, provided:

''[(a) Repealed]

''(b) The Director of the Office of Management and Budget shall delegate to the Administrator for the Office of Information and Regulatory Affairs all functions, authority, and responsibility of the Director under section 552a of title 5, United States Code, under Executive Order 12046 [Ex. Ord. No. 12046, Mar. 27, 1978, 43 F.R. 14193, set out as a note under section 305 of Title 47, Telecommunications] and Reorganization Plan No. 1 for telecommunications [probably means Reorg. Plan No. 1 of 1970, 35 F.R. 6421, 84 Stat. 2083, set out in the Appendix to Title 5, Government Organization and Employees], and under sections 110 and 111 of the Federal Property and Administrative Services Act of 1949 ([former 40 U.S.C. 322 and former] 40 U.S.C. 759).''

[Section 101(m) [title VIII, § 833] of Pub. L. 99–500 and Pub. L. 99–591 provided that: ''This title and the amendments made by this title [amending former sections 3501 to 3507, 3511, 3514, and 3520 of this title and sections 751, 757, and 759 of former Title 40, Public Buildings, Property, and Works, enacting provisions set out as a notes under section 101 of this title and former section 3503 of this title, amending provisions set out as a note above, and repealing provisions set out as a note under section 759 of former Title 40] shall take effect on the date of enactment of this Act [Oct. 18, 1986], except as provided in section 813(b) [set out as a note under former section 3503 of this title] and except that the provisions of section 821 and the amendments made by such section [amending former sections 3503 and 3504 of this title, sections 757 and 759 of former Title 40, and provisions set out as a note above] shall take effect on January 1, 1987.'']

§ 3504. Authority and functions of Director

(a)(1) The Director shall oversee the use of information resources to improve the efficiency and effectiveness of governmental operations to serve agency missions, including burden reduction and service delivery to the public. In performing such oversight, the Director shall—

(A) develop, coordinate and oversee the implementation of Federal information resources management policies, principles, standards, and guidelines; and

(B) provide direction and oversee—

(i) the review and approval of the collection of information and the reduction of the information collection burden;

(ii) agency dissemination of and public access to information;

(iii) statistical activities;

(iv) records management activities;

(v) privacy, confidentiality, security, disclosure, and sharing of information; and

(vi) the acquisition and use of information technology, including alternative information technologies that provide for electronic submission, maintenance, or disclosure of information as a substitute for paper and for the use and acceptance of electronic signatures.

(2) The authority of the Director under this subchapter shall be exercised consistent with applicable law.

(b) With respect to general information resources management policy, the Director shall—

(1) develop and oversee the implementation of uniform information resources management policies, principles, standards, and guidelines;

(2) foster greater sharing, dissemination, and access to public information, including through—

(A) the use of comprehensive data inventories and the Federal data catalogue under section 3511; and

(B) the development and utilization of common standards for information collection, storage, processing and communication, including standards for security, interconnectivity and interoperability;

(3) initiate and review proposals for changes in legislation, regulations, and agency procedures to improve information resources management practices;

(4) oversee the development and implementation of best practices in information resources management, including training;

(5) oversee agency integration of program and management functions with information resources management functions; and

(6) issue guidance for agencies to implement section 3506(b)(6) in a manner that takes into account—

(A) risks and restrictions related to the disclosure of personally identifiable information, including the risk that an individual data asset in isolation does not pose a privacy or confidentiality risk but when combined with other available information may pose such a risk;

(B) security considerations, including the risk that information in an individual data asset in isolation does not pose a security risk but when combined with other available information may pose such a risk;

(C) the cost and benefits to the public of converting a data asset into a machine-readable format that is accessible and useful to the public;

(D) whether the application of the requirements described in such section to a data asset could result in legal liability;

(E) a determination of whether a data asset—

(i) is subject to intellectual property rights, including rights under titles 17 and 35;

(ii) contains confidential business information, that could be withheld under section 552(b)(4) of title 5; or

(iii) is otherwise restricted by contract or other binding, written agreement;

(F) the requirement that a data asset be disclosed, if it would otherwise be made available under section 552 of title 5 (commonly known as the ''Freedom of Information Act''); and

(G) any other considerations that the Director determines to be relevant.

(c) With respect to the collection of information and the control of paperwork, the Director shall—

(1) review and approve proposed agency collections of information;

(2) coordinate the review of the collection of information associated with Federal procurement and acquisition by the Office of Information and Regulatory Affairs with the Office of Federal Procurement Policy, with particular emphasis on applying information technology to improve the efficiency and effectiveness of Federal procurement, acquisition and payment, and to reduce information collection burdens on the public;

(3) minimize the Federal information collection burden, with particular emphasis on those individuals and entities most adversely affected;

(4) maximize the practical utility of and public benefit from information collected by or for the Federal Government;

(5) establish and oversee standards and guidelines by which agencies are to estimate the burden to comply with a proposed collection of information; [1]

(6) publish in the Federal Register and make available on the Internet (in consultation with the Small Business Administration) on an annual basis a list of the compliance assistance resources available to small businesses, with the first such publication occurring not later than 1 year after the date of enactment of the Small Business Paperwork Relief Act of 2002.

(d) With respect to information dissemination, the Director shall develop and oversee the implementation of policies, principles, standards, and guidelines to—

(1) apply to Federal agency dissemination of public information, regardless of the form or format in which such information is disseminated; and

(2) promote public access to public information and fulfill the purposes of this subchapter, including through the effective use of information technology.

(e) With respect to statistical policy and coordination, the Director shall—

(1) coordinate the activities of the Federal statistical system to ensure—

(A) the efficiency and effectiveness of the system; and

(B) the integrity, objectivity, impartiality, utility, and confidentiality of information collected for statistical purposes;

(2) ensure that budget proposals of agencies are consistent with system-wide priorities for maintaining and improving the quality of Federal statistics and prepare an annual report on statistical program funding;

(3) develop and oversee the implementation of Governmentwide policies, principles, standards, and guidelines concerning—

(A) statistical collection procedures and methods;

(B) statistical data classification;

(C) statistical information presentation and dissemination;

(D) timely release of statistical data; and

(E) such statistical data sources as may be required for the administration of Federal programs;

[1] So in original. Probably should be followed by ''and''.

(4) evaluate statistical program performance and agency compliance with Governmentwide policies, principles, standards and guidelines;

(5) promote the sharing of information collected for statistical purposes consistent with privacy rights and confidentiality pledges;

(6) coordinate the participation of the United States in international statistical activities, including the development of comparable statistics;

(7) appoint a chief statistician who is a trained and experienced professional statistician to carry out the functions described under this subsection;

(8) establish an Interagency Council on Statistical Policy to advise and assist the Director in carrying out the functions under this subsection that shall—

(A) be headed by the chief statistician; and

(B) consist of—

(i) the heads of the major statistical programs; and

(ii) representatives of other statistical agencies under rotating membership;

(9) provide opportunities for training in statistical policy functions to employees of the Federal Government under which—

(A) each trainee shall be selected at the discretion of the Director based on agency requests and shall serve under the chief statistician for at least 6 months and not more than 1 year; and

(B) all costs of the training shall be paid by the agency requesting training; and

(10) ensure that any change to the standards of core-based statistical area (as defined in section 4 of the MAPS Act of 2021) delineations pursuant to this subsection shall—

(A) be accompanied by a public report that explains—

(i) the scientific basis, criteria, and methodology for such change to existing standards, including clear quantitative thresholds for determining any future statistical re-delineations; and

(ii) the opinions of domestic and international experts in statistics and demographics, including government experts at the Bureau of the Census and other relevant agencies, who were consulted regarding such change to existing standards;

(B) not be influenced by any non-statistical considerations such as impact on program administration or service delivery; and

(C) not propagate automatically for any non-statistical use by any domestic assistance program (as defined in section 4 of the MAPS Act of 2021).

(f) With respect to records management, the Director shall—

(1) provide advice and assistance to the Archivist of the United States and the Administrator of General Services to promote coordination in the administration of chapters 29, 31, and 33 of this title with the information resources management policies, principles, standards, and guidelines established under this subchapter;

(2) review compliance by agencies with—

(A) the requirements of chapters 29, 31, and 33 of this title; and

(B) regulations promulgated by the Archivist of the United States and the Administrator of General Services; and

(3) oversee the application of records management policies, principles, standards, and guidelines, including requirements for archiving information maintained in electronic format, in the planning and design of information systems.

(g) With respect to privacy and security, the Director shall—

(1) develop and oversee the implementation of policies, principles, standards, and guidelines on privacy, confidentiality, security, disclosure and sharing of information collected or maintained by or for agencies; and

(2) oversee and coordinate compliance with sections 552 and 552a of title 5, sections 20 and 21 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3 and 278g–4), section 11331 of title 40 and subchapter II of this chapter, and related information management laws.

(h) With respect to Federal information technology, the Director shall—

(1) in consultation with the Director of the National Institute of Standards and Technology and the Administrator of General Services—

(A) develop and oversee the implementation of policies, principles, standards, and guidelines for information technology functions and activities of the Federal Government, including periodic evaluations of major information systems; and

(B) oversee the development and implementation of standards under section 11331 of title 40;[2]

(2) monitor the effectiveness of, and compliance with, directives issued under subtitle III of title 40 and directives issued under section 322[2] of title 40;

(3) coordinate the development and review by the Office of Information and Regulatory Affairs of policy associated with Federal procurement and acquisition of information technology with the Office of Federal Procurement Policy;

(4) ensure, through the review of agency budget proposals, information resources management plans and other means—

(A) agency integration of information resources management plans, program plans and budgets for acquisition and use of information technology; and

(B) the efficiency and effectiveness of inter-agency information technology initiatives to improve agency performance and the accomplishment of agency missions; and

(5) promote the use of information technology by the Federal Government to improve the productivity, efficiency, and effectiveness of Federal programs, including through dissemination of public information and the reduction of information collection burdens on the public.

[2] See References in Text note below.

(Added Pub. L. 104–13, § 2, May 22, 1995, 109 Stat. 167; amended Pub. L. 104–106, div. E, title LI, § 5131(e)(1), title LVI, § 5605(b), (c), Feb. 10, 1996, 110 Stat. 688, 700; Pub. L. 105–85, div. A, title X, § 1073(h)(5)(B), (C), Nov. 18, 1997, 111 Stat. 1907; Pub. L. 105–277, div. C, title XVII, § 1702, Oct. 21, 1998, 112 Stat. 2681–749; Pub. L. 106–398, § 1 [[div. A], title X, § 1064(b)], Oct. 30, 2000, 114 Stat. 1654, 1654A–275; Pub. L. 107–198, § 2(a), June 28, 2002, 116 Stat. 729; Pub. L. 107–217, § 3(*l*)(5), Aug. 21, 2002, 116 Stat. 1301; Pub. L. 107–296, title X, § 1005(c)(1), Nov. 25, 2002, 116 Stat. 2272; Pub. L. 107–347, title III, § 305(c)(1), Dec. 17, 2002, 116 Stat. 2960; Pub. L. 115–435, title II, § 202(b), (d)(2)(B), Jan. 14, 2019, 132 Stat. 5535, 5541; Pub. L. 117–219, § 7, Dec. 5, 2022, 136 Stat. 2274.)

Editorial Notes

REFERENCES IN TEXT

The date of enactment of the Small Business Paperwork Relief Act of 2002, referred to in subsec. (c)(6), is the date of enactment of Pub. L. 107–198, which was approved June 28, 2002.

Section 4 of the MAPS Act of 2021, referred to in subsec. (e)(10), is section 4 of Pub. L. 117–219, which is set out as a note under section 6102 of Title 31, Money and Finance.

The text of section 11331 of title 40, referred to in subsec. (h)(1)(B), was generally amended by Pub. L. 117–167, div. B, title II, § 10246(f), Aug. 9, 2022, 136 Stat. 1492, so as to provide for the prescription by the Secretary of Commerce of standards and guidelines pertaining to Federal information systems.

Section 322 of title 40, referred to in subsec. (h)(2), was repealed by Pub. L. 109–313, § 3(h)(1), Oct. 6, 2006, 120 Stat. 1736.

PRIOR PROVISIONS

A prior section 3504, added Pub. L. 96–511, § 2(a), Dec. 11, 1980, 94 Stat. 2815; amended Pub. L. 98–497, title I, § 107(b)(26), Oct. 19, 1984, 98 Stat. 2291; Pub. L. 99–500, § 101(m) [title VIII, §§ 814, 821(b)(2)], Oct. 18, 1986, 100 Stat. 1783–308, 1783–336, 1783–342, and Pub. L. 99–591, § 101(m) [title VIII, §§ 814, 821(b)(2)], Oct. 30, 1986, 100 Stat. 3341–308, 3341–336, 3341–342, related to authority and functions of Director prior to the general amendment of this chapter by Pub. L. 104–13.

Another prior section 3504, Pub. L. 90–620, Oct. 22, 1968, 82 Stat. 1303, provided for designation of a central collection agency, prior to the general amendment of this chapter by Pub. L. 96–511. See section 3509 of this title.

AMENDMENTS

2022—Subsec. (e)(10). Pub. L. 117–219 added par. (10).

2019—Subsec. (b)(2)(A). Pub. L. 115–435, § 202(d)(2)(B), substituted ''the use of comprehensive data inventories and the Federal data catalogue under section 3511'' for ''the use of the Government Information Locator Service''.

Subsec. (b)(6). Pub. L. 115–435, § 202(b), added par. (6).

2002—Subsec. (c)(6). Pub. L. 107–198 added par. (6).

Subsec. (g)(1). Pub. L. 107–296, § 1005(c)(1)(A), and Pub. L. 107–347, § 305(c)(1)(A), amended par. (1) identically, inserting ''and'' at end.

Subsec. (g)(2). Pub. L. 107–347, § 305(c)(1)(B), substituted ''section 11331 of title 40 and subchapter II of this chapter'' for ''sections 11331 and 11332(b) and (c) of title 40'' and a period for ''; and'' at end.

Pub. L. 107–296, § 1005(c)(1)(B), which directed amendment of par. (2) by substituting ''section 11331 of title 40 and subchapter II of this title'' for ''sections 11331 and 11332(b) and (c) of title 40'' and a period for the semicolon, could not be executed because of amendment by Pub. L. 107–347, § 305(c)(1)(B). See Amendment note above and Effective Date of 2002 Amendments notes below.

Pub. L. 107–217, § 3(*l*)(5)(A), substituted ''sections 11331 and 11332(b) and (c) of title 40'' for ''section 5131 of the Clinger-Cohen Act of 1996 (40 U.S.C. 1441), and sections 5 and 6 of the Computer Security Act of 1987 (40 U.S.C. 759 note)''.

Subsec. (g)(3). Pub. L. 107–296, § 1005(c)(1)(C), and Pub. L. 107–347, § 305(c)(1)(C), amended subsec. (g) identically, striking out par. (3) which read as follows: ''require Federal agencies, consistent with the standards and guidelines promulgated under sections 11331 and 11332(b) and (c) of title 40, to identify and afford security protections commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of information collected or maintained by or on behalf of an agency.''

Pub. L. 107–217, § 3(*l*)(5)(B), substituted ''sections 11331 and 11332(b) and (c) of title 40'' for ''section 5131 of the Clinger-Cohen Act of 1996 (40 U.S.C. 1441) and sections 5 and 6 of the Computer Security Act of 1987 (40 U.S.C. 759 note)''.

Subsec. (h)(1)(B). Pub. L. 107–217, § 3(*l*)(5)(C), substituted ''section 11331 of title 40'' for ''section 5131 of the Clinger-Cohen Act of 1996 (40 U.S.C. 1441)''.

Subsec. (h)(2). Pub. L. 107–217, § 3(*l*)(5)(D), substituted ''subtitle III of title 40'' for ''division E of the Clinger-Cohen Act of 1996 (40 U.S.C. 1401 et seq.)'' and ''section 322 of title 40'' for ''section 110 of the Federal Property and Administrative Services Act of 1949 (40 U.S.C. 757)''.

2000—Subsecs. (a)(2), (d)(2), (f)(1). Pub. L. 106–398 substituted ''subchapter'' for ''chapter''.

1998—Subsec. (a)(1)(B)(vi). Pub. L. 105–277 amended cl. (vi) generally. Prior to amendment, cl. (vi) read as follows: ''the acquisition and use of information technology.''

1997—Subsecs. (g)(2), (3), (h)(1)(B). Pub. L. 105–85, § 1073(h)(5)(C), substituted ''Clinger-Cohen Act of 1996 (40 U.S.C. 1441)'' for ''Information Technology Management Reform Act of 1996''.

Subsec. (h)(2). Pub. L. 105–85, § 1073(h)(5)(B), substituted ''division E of the Clinger-Cohen Act of 1996 (40 U.S.C. 1401 et seq.)'' for ''the Information Technology Management Reform Act of 1996''.

1996—Subsec. (g)(2). Pub. L. 104–106, § 5131(e)(1)(A), substituted ''sections 20 and 21 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3 and 278g–4), section 5131 of the Information Technology Management Reform Act of 1996, and sections 5 and 6 of the Computer Security Act of 1987 (40 U.S.C. 759 note)'' for ''the Computer Security Act of 1987 (40 U.S.C. 759 note)''.

Subsec. (g)(3). Pub. L. 104–106, § 5131(e)(1)(B), substituted ''the standards and guidelines promulgated under section 5131 of the Information Technology Management Reform Act of 1996 and sections 5 and 6 of the Computer Security Act of 1987 (40 U.S.C. 759 note)'' for ''the Computer Security Act of 1987 (40 U.S.C. 759 note)''.

Subsec. (h)(1)(B). Pub. L. 104–106, § 5605(b), substituted ''section 5131 of the Information Technology Management Reform Act of 1996'' for ''section 111(d) of the Federal Property and Administrative Services Act of 1949 (40 U.S.C. 759(d))''.

Subsec. (h)(2). Pub. L. 104–106, § 5605(c), substituted ''the Information Technology Management Reform Act of 1996 and directives issued under section 110 of the Federal Property and Administrative Services Act of 1949 (40 U.S.C. 757)'' for ''sections 110 and 111 of the Federal Property and Administrative Services Act of 1949 (40 U.S.C. 757 and 759)''.

Statutory Notes and Related Subsidiaries

EFFECTIVE DATE OF 2019 AMENDMENT

Amendment by Pub. L. 115–435 effective 180 days after Jan. 14, 2019, see section 403 of Pub. L. 115–435, set out as a note under section 306 of Title 5, Government Organization and Employees.

EFFECTIVE DATE OF 2002 AMENDMENTS

Pub. L. 107–347, title IV, § 402(b), Dec. 17, 2002, 116 Stat. 2962, provided that: ''Title III [see Short Title of 2002

Amendments note set out under section 101 of this title] and this title [enacting provisions set out as a note under section 3601 of this title] shall take effect on the date of enactment of this Act [Dec. 17, 2002].''

Amendment by Pub. L. 107–296 effective 60 days after Nov. 25, 2002, see section 4 of Pub. L. 107–296, set out as an Effective Date note under section 101 of Title 6, Domestic Security.

EFFECTIVE DATE OF 2000 AMENDMENT

Amendment by Pub. L. 106–398 effective 30 days after Oct. 30, 2000, see section 1 [[div. A], title X, §1065] of Pub. L. 106–398, Oct. 30, 2000, 114 Stat. 1654, formerly set out as an Effective Date note under former section 3531 of this title.

EFFECTIVE DATE OF 1996 AMENDMENT

Amendment by Pub. L. 104–106 effective 180 days after Feb. 10, 1996, see section 5701 of Pub. L. 104–106, Feb. 10, 1996, 110 Stat. 702.

EFFECTIVE DATE

Section effective Oct. 1, 1995, except as otherwise provided, see section 4(a) of Pub. L. 104–13, set out as a note under section 3501 of this title.

GOVERNMENT PAPERWORK ELIMINATION

Pub. L. 105–277, div. C, title XVII, Oct. 21, 1998, 112 Stat. 2681–749, provided that:

''SEC. 1701. SHORT TITLE.

''This title may be cited as the 'Government Paperwork Elimination Act'.

''SEC. 1702. AUTHORITY OF OMB TO PROVIDE FOR ACQUISITION AND USE OF ALTERNATIVE INFORMATION TECHNOLOGIES BY EXECUTIVE AGENCIES.

''[Amended this section.]

''SEC. 1703. PROCEDURES FOR USE AND ACCEPTANCE OF ELECTRONIC SIGNATURES BY EXECUTIVE AGENCIES.

''(a) IN GENERAL.—In order to fulfill the responsibility to administer the functions assigned under chapter 35 of title 44, United States Code, the provisions of the Clinger-Cohen Act of 1996 (divisions D and E of Public Law 104–106) [see Short Title of 1996 Act note set out under section 101 of Title 41, Public Contracts] and the amendments made by that Act, and the provisions of this title, the Director of the Office of Management and Budget shall, in consultation with the National Telecommunications and Information Administration and not later than 18 months after the date of enactment of this Act [Oct. 21, 1998], develop procedures for the use and acceptance of electronic signatures by Executive agencies.

''(b) REQUIREMENTS FOR PROCEDURES.—(1) The procedures developed under subsection (a)—

''(A) shall be compatible with standards and technology for electronic signatures that are generally used in commerce and industry and by State governments;

''(B) may not inappropriately favor one industry or technology;

''(C) shall ensure that electronic signatures are as reliable as is appropriate for the purpose in question and keep intact the information submitted;

''(D) shall provide for the electronic acknowledgment of electronic forms that are successfully submitted; and

''(E) shall, to the extent feasible and appropriate, require an Executive agency that anticipates receipt by electronic means of 50,000 or more submittals of a particular form to take all steps necessary to ensure that multiple methods of electronic signatures are available for the submittal of such form.

''(2) The Director shall ensure the compatibility of the procedures under paragraph (1)(A) in consultation with appropriate private bodies and State government entities that set standards for the use and acceptance of electronic signatures.

''SEC. 1704. DEADLINE FOR IMPLEMENTATION BY EXECUTIVE AGENCIES OF PROCEDURES FOR USE AND ACCEPTANCE OF ELECTRONIC SIGNATURES.

''In order to fulfill the responsibility to administer the functions assigned under chapter 35 of title 44, United States Code, the provisions of the Clinger-Cohen Act of 1996 (divisions D and E of Public Law 104–106) [see Short Title of 1996 Act note set out under section 101 of Title 41] and the amendments made by that Act, and the provisions of this title, the Director of the Office of Management and Budget shall ensure that, commencing not later than five years after the date of enactment of this Act [Oct. 21, 1998], Executive agencies provide—

''(1) for the option of the electronic maintenance, submission, or disclosure of information, when practicable as a substitute for paper; and

''(2) for the use and acceptance of electronic signatures, when practicable.

''SEC. 1705. ELECTRONIC STORAGE AND FILING OF EMPLOYMENT FORMS.

''In order to fulfill the responsibility to administer the functions assigned under chapter 35 of title 44, United States Code, the provisions of the Clinger-Cohen Act of 1996 (divisions D and E of Public Law 104–106) [see Short Title of 1996 Amendment Act set out under section 101 of Title 41] and the amendments made by that Act, and the provisions of this title, the Director of the Office of Management and Budget shall, not later than 18 months after the date of enactment of this Act [Oct. 21, 1998], develop procedures to permit private employers to store and file electronically with Executive agencies forms containing information pertaining to the employees of such employers.

''SEC. 1706. STUDY ON USE OF ELECTRONIC SIGNATURES.

''(a) ONGOING STUDY REQUIRED.—In order to fulfill the responsibility to administer the functions assigned under chapter 35 of title 44, United States Code, the provisions of the Clinger-Cohen Act of 1996 (divisions D and E of Public Law 104–106) [see Short Title of 1996 Act note set out under section 101 of Title 41] and the amendments made by that Act, and the provisions of this title, the Director of the Office of Management and Budget shall, in cooperation with the National Telecommunications and Information Administration, conduct an ongoing study of the use of electronic signatures under this title on—

''(1) paperwork reduction and electronic commerce;

''(2) individual privacy; and

''(3) the security and authenticity of transactions.

''(b) REPORTS.—The Director shall submit to Congress on a periodic basis a report describing the results of the study carried out under subsection (a).

''SEC. 1707. ENFORCEABILITY AND LEGAL EFFECT OF ELECTRONIC RECORDS.

''Electronic records submitted or maintained in accordance with procedures developed under this title, or electronic signatures or other forms of electronic authentication used in accordance with such procedures, shall not be denied legal effect, validity, or enforceability because such records are in electronic form.

''SEC. 1708. DISCLOSURE OF INFORMATION.

''Except as provided by law, information collected in the provision of electronic signature services for communications with an executive agency, as provided by this title, shall only be used or disclosed by persons who obtain, collect, or maintain such information as a business or government practice, for the purpose of facilitating such communications, or with the prior affirmative consent of the person about whom the information pertains.

''SEC. 1709. APPLICATION WITH INTERNAL REVENUE LAWS.

''No provision of this title shall apply to the Department of the Treasury or the Internal Revenue Service to the extent that such provision—

''(1) involves the administration of the internal revenue laws; or

''(2) conflicts with any provision of the Internal Revenue Service Restructuring and Reform Act of 1998 [Pub. L. 105–206, see Tables for classification] or the Internal Revenue Code of 1986 [26 U.S.C. 1 et seq.].

''SEC. 1710. DEFINITIONS.

''For purposes of this title:

''(1) ELECTRONIC SIGNATURE.—The term 'electronic signature' means a method of signing an electronic message that—

''(A) identifies and authenticates a particular person as the source of the electronic message; and

''(B) indicates such person's approval of the information contained in the electronic message.

''(2) EXECUTIVE AGENCY.—The term 'Executive agency' has the meaning given that term in section 105 of title 5, United States Code.''

§ 3505. Assignment of tasks and deadlines

(a) In carrying out the functions under this subchapter, the Director shall—

(1) in consultation with agency heads, set an annual Governmentwide goal for the reduction of information collection burdens by at least 10 percent during each of fiscal years 1996 and 1997 and 5 percent during each of fiscal years 1998, 1999, 2000, and 2001, and set annual agency goals to—

(A) reduce information collection burdens imposed on the public that—

(i) represent the maximum practicable opportunity in each agency; and

(ii) are consistent with improving agency management of the process for the review of collections of information established under section 3506(c); and

(B) improve information resources management in ways that increase the productivity, efficiency and effectiveness of Federal programs, including service delivery to the public;

(2) with selected agencies and non-Federal entities on a voluntary basis, conduct pilot projects to test alternative policies, practices, regulations, and procedures to fulfill the purposes of this subchapter, particularly with regard to minimizing the Federal information collection burden; and

(3) in consultation with the Administrator of General Services, the Director of the National Institute of Standards and Technology, the Archivist of the United States, and the Director of the Office of Personnel Management, develop and maintain a Governmentwide strategic plan for information resources management, that shall include—

(A) a description of the objectives and the means by which the Federal Government shall apply information resources to improve agency and program performance;

(B) plans for—

(i) reducing information burdens on the public, including reducing such burdens through the elimination of duplication and meeting shared data needs with shared resources;

(ii) enhancing public access to and dissemination of, information, using electronic and other formats; and

(iii) meeting the information technology needs of the Federal Government in accordance with the purposes of this subchapter; and

(C) a description of progress in applying information resources management to improve agency performance and the accomplishment of missions.

(b) For purposes of any pilot project conducted under subsection (a)(2), the Director may, after consultation with the agency head, waive the application of any administrative directive issued by an agency with which the project is conducted, including any directive requiring a collection of information, after giving timely notice to the public and the Congress regarding the need for such waiver.

(c)[1] INVENTORY OF MAJOR INFORMATION SYSTEMS.—(1) The head of each agency shall develop and maintain an inventory of major information systems (including major national security systems) operated by or under the control of such agency.

(2) The identification of information systems in an inventory under this subsection shall include an identification of the interfaces between each such system and all other systems or networks, including those not operated by or under the control of the agency.

(3) Such inventory shall be—

(A) updated at least annually;

(B) made available to the Comptroller General; and

(C) used to support information resources management, including—

(i) preparation and maintenance of the inventory of information resources under section 3506(b)(4);

(ii) information technology planning, budgeting, acquisition, and management under section 3506(h), subtitle III of title 40, and related laws and guidance;

(iii) monitoring, testing, and evaluation of information security controls under subchapter II;

(iv) preparation of the index of major information systems required under section 552(g) of title 5, United States Code; and

(v) preparation of information system inventories required for records management under chapters 21, 29, 31, and 33.

(4) The Director shall issue guidance for and oversee the implementation of the requirements of this subsection.

(c)[1] INVENTORY OF INFORMATION SYSTEMS.—(1) The head of each agency shall develop and maintain an inventory of the information systems (including national security systems) operated by or under the control of such agency;

(2) The identification of information systems in an inventory under this subsection shall include an identification of the interfaces between each such system and all other systems or networks, including those not operated by or under the control of the agency;

[1] So in original. Two subsecs. (c) have been enacted.

(3) Such inventory shall be—

(A) updated at least annually;

(B) made available to the Comptroller General; and

(C) used to support information resources management, including—

(i) preparation and maintenance of the inventory of information resources under section 3506(b)(4);

(ii) information technology planning, budgeting, acquisition, and management under section 3506(h), subtitle III of title 40, and related laws and guidance;

(iii) monitoring, testing, and evaluation of information security controls under subchapter II;

(iv) preparation of the index of major information systems required under section 552(g) of title 5, United States Code; and

(v) preparation of information system inventories required for records management under chapters 21, 29, 31, and 33.

(4) The Director shall issue guidance for and oversee the implementation of the requirements of this subsection.

(Added Pub. L. 104–13, § 2, May 22, 1995, 109 Stat. 170; amended Pub. L. 106–398, § 1 [[div. A], title X, § 1064(b)], Oct. 30, 2000, 114 Stat. 1654, 1654A–275; Pub. L. 107–296, title X, § 1005(c)(2), Nov. 25, 2002, 116 Stat. 2272; Pub. L. 107–347, title III, § 305(c)(2), Dec. 17, 2002, 116 Stat. 2961.)

Editorial Notes

PRIOR PROVISIONS

A prior section 3505, added Pub. L. 96–511, § 2(a), Dec. 11, 1980, 94 Stat. 2818; amended Pub. L. 99–500, § 101(m) [title VIII, § 815], Oct. 18, 1986, 100 Stat. 1783–308, 1783–337, and Pub. L. 99–591, § 101(m) [title VIII, § 815], Oct. 30, 1986, 100 Stat. 3341–308, 3341–337, related to assignment of tasks and deadlines prior to the general amendment of this chapter by Pub. L. 104–13.

Another prior section 3505, Pub. L. 90–620, Oct. 22, 1968, 82 Stat. 1303, prohibited independent collection by an agency, prior to the general amendment of this chapter by Pub. L. 96–511. See section 3509 of this title.

AMENDMENTS

2002—Subsec. (c). Pub. L. 107–347, added subsec. (c) relating to inventory of major information systems.

Pub. L. 107–296 added subsec. (c) relating to inventory of information systems.

2000—Subsec. (a). Pub. L. 106–398 substituted ''subchapter'' for ''chapter'' in introductory provisions and pars. (2) and (3)(B)(iii).

Statutory Notes and Related Subsidiaries

EFFECTIVE DATE OF 2002 AMENDMENT

Amendment by Pub. L. 107–347 effective Dec. 17, 2002, see section 402(b) of Pub. L. 107–347, set out as a note under section 3504 of this title.

Amendment by Pub. L. 107–296 effective 60 days after Nov. 25, 2002, see section 4 of Pub. L. 107–296, set out as an Effective Date note under section 101 of Title 6, Domestic Security.

EFFECTIVE DATE OF 2000 AMENDMENT

Amendment by Pub. L. 106–398 effective 30 days after Oct. 30, 2000, see section 1 [[div. A], title X, § 1065] of Pub. L. 106–398, Oct. 30, 2000, 114 Stat. 1654, formerly set out as an Effective Date note under former section 3531 of this title.

EFFECTIVE DATE

Section effective Oct. 1, 1995, except as otherwise provided, see section 4(a) of Pub. L. 104–13, set out as a note under section 3501 of this title.

§ 3506. Federal agency responsibilities

(a)(1) The head of each agency shall be responsible for—

(A) carrying out the agency's information resources management activities to improve agency productivity, efficiency, and effectiveness; and

(B) complying with the requirements of this subchapter and related policies established by the Director.

(2)(A) Except as provided under subparagraph (B), the head of each agency shall designate a Chief Information Officer who shall report directly to such agency head to carry out the responsibilities of the agency under this subchapter.

(B) The Secretary of the Department of Defense and the Secretary of each military department may each designate Chief Information Officers who shall report directly to such Secretary to carry out the responsibilities of the department under this subchapter. If more than one Chief Information Officer is designated, the respective duties of the Chief Information Officers shall be clearly delineated.

(3) The Chief Information Officer designated under paragraph (2) shall head an office responsible for ensuring agency compliance with and prompt, efficient, and effective implementation of the information policies and information resources management responsibilities established under this subchapter, including the reduction of information collection burdens on the public. The Chief Information Officer and employees of such office shall be selected with special attention to the professional qualifications required to administer the functions described under this subchapter.

(4) Each agency program official shall be responsible and accountable for information resources assigned to and supporting the programs under such official. In consultation with the Chief Information Officer designated under paragraph (2) and the agency Chief Financial Officer (or comparable official), each agency program official shall define program information needs and develop strategies, systems, and capabilities to meet those needs.

(b) With respect to general information resources management, each agency shall—

(1) manage information resources to—

(A) reduce information collection burdens on the public;

(B) increase program efficiency and effectiveness; and

(C) improve the integrity, quality, and utility of information to all users within and outside the agency, including capabilities for ensuring dissemination of public information, public access to government information, and protections for privacy and security;

(2) in accordance with guidance by the Director, develop and maintain a strategic information resources management plan that, to the extent practicable—

(A) describes how information resources management activities help accomplish agency missions;

(B) includes an open data plan for data that does not concern monetary policy that—

(i) requires the agency to develop processes and procedures that—

(I) require data collection mechanisms created on or after the date of the enactment of the OPEN Government Data Act to be available in an open format; and

(II) facilitate collaboration with non-Government entities (including businesses), researchers, and the public for the purpose of understanding how data users value and use government data;

(ii) identifies and implements methods for collecting and analyzing digital information on data asset usage by users within and outside of the agency, including designating a point of contact within the agency to assist the public and to respond to quality issues, usability issues, recommendations for improvements, and complaints about adherence to open data requirements within a reasonable period of time;

(iii) develops and implements a process to evaluate and improve the timeliness, completeness, consistency, accuracy, usefulness, and availability of open Government data assets;

(iv) includes requirements for meeting the goals of the agency open data plan, including the acquisition of technology, provision of training for employees, and the implementation of procurement standards, in accordance with existing law, regulation, and policy, that allow for the acquisition of innovative solutions from public and private sectors;

(v) identifies as priority data assets any data asset for which disclosure would be in the public interest and establishes a plan to evaluate each priority data asset for disclosure on the Federal Data Catalogue under section 3511 and for a determination under[1] 3511(a)(2)(A)(iii)(I)(bb), including an accounting of which priority data assets have not yet been evaluated; and

(vi) requires the agency to comply with requirements under section 3511, including any standards established by the Director under such section, when disclosing a data asset pursuant to such section; and

(C) is updated annually and made publicly available on the website of the agency not later than 5 days after each such update;

(3) develop and maintain an ongoing process to—

(A) ensure that information resources management operations and decisions are integrated with organizational planning, budget, financial management, human resources management, and program decisions;

(B) in cooperation with the agency Chief Financial Officer (or comparable official), develop a full and accurate accounting of information technology expenditures, related expenses, and results; and

(C) establish goals for improving information resources management's contribution to program productivity, efficiency, and effectiveness, methods for measuring progress towards those goals, and clear roles and responsibilities for achieving those goals;

(4) in consultation with the Director, the Administrator of General Services, and the Archivist of the United States, maintain a current and complete inventory of the agency's information resources, including directories necessary to fulfill the requirements of section 3511 of this subchapter;

(5) in consultation with the Director and the Director of the Office of Personnel Management, conduct formal training programs to educate agency program and management officials about information resources management; and

(6) in accordance with guidance by the Director—

(A) make each data asset of the agency available in an open format; and

(B) make each public data asset of the agency available—

(i) as an open Government data asset; and

(ii) under an open license.

(c) With respect to the collection of information and the control of paperwork, each agency shall—

(1) establish a process within the office headed by the Chief Information Officer designated under subsection (a), that is sufficiently independent of program responsibility to evaluate fairly whether proposed collections of information should be approved under this subchapter, to—

(A) review each collection of information before submission to the Director for review under this subchapter, including—

(i) an evaluation of the need for the collection of information;

(ii) a functional description of the information to be collected;

(iii) a plan for the collection of the information;

(iv) a specific, objectively supported estimate of burden;

(v) a test of the collection of information through a pilot program, if appropriate; and

(vi) a plan for the efficient and effective management and use of the information to be collected, including necessary resources;

(B) ensure that each information collection—

(i) is inventoried, displays a control number and, if appropriate, an expiration date;

(ii) indicates the collection is in accordance with the clearance requirements of section 3507; and

(iii) informs the person receiving the collection of information of—

(I) the reasons the information is being collected;

[1] So in original. Probably should be followed by ''section''.

(II) the way such information is to be used;

(III) an estimate, to the extent practicable, of the burden of the collection;

(IV) whether responses to the collection of information are voluntary, required to obtain a benefit, or mandatory; and

(V) the fact that an agency may not conduct or sponsor, and a person is not required to respond to, a collection of information unless it displays a valid control number; and

(C) assess the information collection burden of proposed legislation affecting the agency;

(2)(A) except as provided under subparagraph (B) or section 3507(j), provide 60-day notice in the Federal Register, and otherwise consult with members of the public and affected agencies concerning each proposed collection of information, to solicit comment to—

(i) evaluate whether the proposed collection of information is necessary for the proper performance of the functions of the agency, including whether the information shall have practical utility;

(ii) evaluate the accuracy of the agency's estimate of the burden of the proposed collection of information;

(iii) enhance the quality, utility, and clarity of the information to be collected; and

(iv) minimize the burden of the collection of information on those who are to respond, including through the use of automated collection techniques or other forms of information technology; and

(B) for any proposed collection of information contained in a proposed rule (to be reviewed by the Director under section 3507(d)), provide notice and comment through the notice of proposed rulemaking for the proposed rule and such notice shall have the same purposes specified under subparagraph (A)(i) through (iv);

(3) certify (and provide a record supporting such certification, including public comments received by the agency) that each collection of information submitted to the Director for review under section 3507—

(A) is necessary for the proper performance of the functions of the agency, including that the information has practical utility;

(B) is not unnecessarily duplicative of information otherwise reasonably accessible to the agency;

(C) reduces to the extent practicable and appropriate the burden on persons who shall provide information to or for the agency, including with respect to small entities, as defined under section 601(6) of title 5, the use of such techniques as—

(i) establishing differing compliance or reporting requirements or timetables that take into account the resources available to those who are to respond;

(ii) the clarification, consolidation, or simplification of compliance and reporting requirements; or

(iii) an exemption from coverage of the collection of information, or any part thereof;

(D) is written using plain, coherent, and unambiguous terminology and is understandable to those who are to respond;

(E) is to be implemented in ways consistent and compatible, to the maximum extent practicable, with the existing reporting and recordkeeping practices of those who are to respond;

(F) indicates for each recordkeeping requirement the length of time persons are required to maintain the records specified;

(G) contains the statement required under paragraph (1)(B)(iii);

(H) has been developed by an office that has planned and allocated resources for the efficient and effective management and use of the information to be collected, including the processing of the information in a manner which shall enhance, where appropriate, the utility of the information to agencies and the public;

(I) uses effective and efficient statistical survey methodology appropriate to the purpose for which the information is to be collected; and

(J) to the maximum extent practicable, uses information technology to reduce burden and improve data quality, agency efficiency and responsiveness to the public; and

(4) in addition to the requirements of this chapter regarding the reduction of information collection burdens for small business concerns (as defined in section 3 of the Small Business Act (15 U.S.C. 632)), make efforts to further reduce the information collection burden for small business concerns with fewer than 25 employees.

(d) With respect to information dissemination, each agency shall—

(1) ensure that the public has timely and equitable access to the agency's public information, including ensuring such access through—

(A) encouraging a diversity of public and private sources for information based on government public information;

(B) in cases in which the agency provides public information maintained in electronic format, providing timely and equitable access to the underlying data (in whole or in part); and

(C) agency dissemination of public information in an efficient, effective, and economical manner;

(2) regularly solicit and consider public input on the agency's information dissemination activities;

(3) provide adequate notice when initiating, substantially modifying, or terminating significant information dissemination products;

(4) not, except where specifically authorized by statute—

(A) establish an exclusive, restricted, or other distribution arrangement that interferes with timely and equitable availability of public information to the public;

(B) restrict or regulate the use, resale, or redissemination of public information by the public;

(C) charge fees or royalties for resale or redissemination of public information; or

(D) establish user fees for public information that exceed the cost of dissemination;

(5) ensure that any public data asset of the agency is machine-readable; and

(6) engage the public in using public data assets of the agency and encourage collaboration by—

(A) publishing on the website of the agency, on a regular basis (not less than annually), information on the usage of such assets by non-Government users;

(B) providing the public with the opportunity to request specific data assets to be prioritized for disclosure and to provide suggestions for the development of agency criteria with respect to prioritizing data assets for disclosure;

(C) assisting the public in expanding the use of public data assets; and

(D) hosting challenges, competitions, events, or other initiatives designed to create additional value from public data assets of the agency.

(e) With respect to statistical policy and coordination, each agency shall—

(1) ensure the relevance, accuracy, timeliness, integrity, and objectivity of information collected or created for statistical purposes;

(2) inform respondents fully and accurately about the sponsors, purposes, and uses of statistical surveys and studies;

(3) protect respondents' privacy and ensure that disclosure policies fully honor pledges of confidentiality;

(4) observe Federal standards and practices for data collection, analysis, documentation, sharing, and dissemination of information;

(5) ensure the timely publication of the results of statistical surveys and studies, including information about the quality and limitations of the surveys and studies; and

(6) make data available to statistical agencies and readily accessible to the public.

(f) With respect to records management, each agency shall implement and enforce applicable policies and procedures, including requirements for archiving information maintained in electronic format, particularly in the planning, design and operation of information systems.

(g) With respect to privacy and security, each agency shall—

(1) implement and enforce applicable policies, procedures, standards, and guidelines on privacy, confidentiality, security, disclosure and sharing of information collected or maintained by or for the agency; and

(2) assume responsibility and accountability for compliance with and coordinated management of sections 552 and 552a of title 5, subchapter II of this chapter, and related information management laws.

(h) With respect to Federal information technology, each agency shall—

(1) implement and enforce applicable Governmentwide and agency information technology management policies, principles, standards, and guidelines;

(2) assume responsibility and accountability for information technology investments;

(3) promote the use of information technology by the agency to improve the productivity, efficiency, and effectiveness of agency programs, including the reduction of information collection burdens on the public and improved dissemination of public information;

(4) propose changes in legislation, regulations, and agency procedures to improve information technology practices, including changes that improve the ability of the agency to use technology to reduce burden; and

(5) assume responsibility for maximizing the value and assessing and managing the risks of major information systems initiatives through a process that is—

(A) integrated with budget, financial, and program management decisions; and

(B) used to select, control, and evaluate the results of major information systems initiatives.

(i)(1) In addition to the requirements described in subsection (c), each agency shall, with respect to the collection of information and the control of paperwork, establish 1 point of contact in the agency to act as a liaison between the agency and small business concerns (as defined in section 3 of the Small Business Act (15 U.S.C. 632)).

(2) Each point of contact described under paragraph (1) shall be established not later than 1 year after the date of enactment of the Small Business Paperwork Relief Act of 2002.

(Added Pub. L. 104–13, §2, May 22, 1995, 109 Stat. 171; amended Pub. L. 104–106, div. E, title LI, §5125(a), Feb. 10, 1996, 110 Stat. 684; Pub. L. 106–398, §1 [[div. A], title X, §1064(b)], Oct. 30, 2000, 114 Stat. 1654, 1654A–275; Pub. L. 107–198, §2(b), (c), June 28, 2002, 116 Stat. 729; Pub. L. 107–217, §3(*l*)(6), Aug. 21, 2002, 116 Stat. 1302; Pub. L. 107–296, title X, §1005(c)(3), Nov. 25, 2002, 116 Stat. 2273; Pub. L. 107–347, title III, §305(c)(3), Dec. 17, 2002, 116 Stat. 2961; Pub. L. 115–435, title II, §202(c)(1), Jan. 14, 2019, 132 Stat. 5536.)

Editorial Notes

REFERENCES IN TEXT

The date of the enactment of the OPEN Government Data Act, referred to in subsec. (b)(2)(B)(i)(I), is the date of enactment of title II of Pub. L. 115–435, which was approved Jan. 14, 2019.

The date of enactment of the Small Business Paperwork Relief Act of 2002, referred to in subsec. (i)(2), is the date of enactment of Pub. L. 107–198, which was approved June 28, 2002.

PRIOR PROVISIONS

A prior section 3506, added Pub. L. 96–511, §2(a), Dec. 11, 1980, 94 Stat. 2819; amended Pub. L. 99–500, §101(m) [title VIII, §816], Oct. 18, 1986, 100 Stat. 1783–308, 1783–338, and Pub. L. 99–591, §101(m) [title VIII, §816], Oct. 30, 1986, 100 Stat. 3341–308, 3341–338, related to Federal agency responsibilities prior to the general amendment of this chapter by Pub. L. 104–13.

Another prior section 3506, Pub. L. 90–620, Oct. 22, 1968, 82 Stat. 1303, provided for determination of necessity for information and hearing thereon, prior to the general amendment of this chapter by Pub. L. 96–511. See section 3508 of this title.

AMENDMENTS

2019—Subsec. (b)(2). Pub. L. 115–435, §202(c)(1)(A)(i), amended par. (2) generally. Prior to amendment, par.

(2) read as follows: ''in accordance with guidance by the Director, develop and maintain a strategic information resources management plan that shall describe how information resources management activities help accomplish agency missions;''.

Subsec. (b)(6). Pub. L. 115–435, § 202(c)(1)(A)(ii)–(iv), added par. (6).

Subsec. (d)(5), (6). Pub. L. 115–435, § 202(c)(1)(B), added pars. (5) and (6).

2002—Subsec. (c)(4). Pub. L. 107–198, § 2(c), added par. (4).

Subsec. (g)(1). Pub. L. 107–296, § 1005(c)(3)(A), and Pub. L. 107–347, § 305(c)(3)(A), amended par. (1) identically, inserting ''and'' at end.

Subsec. (g)(2). Pub. L. 107–296, § 1005(c)(3)(B), and Pub. L. 107–347, § 305(c)(3)(B), amended par. (2) identically, substituting ''subchapter II of this chapter'' for ''section 11332 of title 40'' and a period for ''; and'' at end.

Pub. L. 107–217, § 3(*l*)(6)(A), substituted ''section 11332 of title 40'' for ''the Computer Security Act of 1987 (40 U.S.C. 759 note)''.

Subsec. (g)(3). Pub. L. 107–296, § 1005(c)(3)(C), and Pub. L. 107–347, § 305(c)(3)(C), amended subsec. (g) identically, striking out par. (3) which read as follows: ''consistent with section 11332 of title 40, identify and afford security protections commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of information collected or maintained by or on behalf of an agency.''

Pub. L. 107–217, § 3(*l*)(6)(B), substituted ''section 11332 of title 40'' for ''the Computer Security Act of 1987 (40 U.S.C. 759 note)''.

Subsec. (i). Pub. L. 107–198, § 2(b), added subsec. (i).

2000—Subsecs. (a)(1) to (3), (b)(4), (c)(1). Pub. L. 106–398 substituted ''subchapter'' for ''chapter'' wherever appearing.

1996—Subsec. (a)(2)(A). Pub. L. 104–106, § 5125(a)(1)(A), substituted ''Chief Information Officer'' for ''senior official''.

Subsec. (a)(2)(B). Pub. L. 104–106, § 5125(a)(1)(B), substituted ''designate Chief Information Officers'' for ''designate senior officials'', ''Chief Information Officer'' for ''official'', and ''the Chief Information Officers'' for ''the officials''.

Subsec. (a)(3), (4). Pub. L. 104–106, § 5125(a)(1)(C), substituted ''Chief Information Officer'' for ''senior official'' wherever appearing.

Subsec. (c)(1). Pub. L. 104–106, § 5125(a)(2), substituted ''Chief Information Officer'' for ''official'' in introductory provisions.

Statutory Notes and Related Subsidiaries

EFFECTIVE DATE OF 2019 AMENDMENT

Pub. L. 115–435, title II, § 202(c)(3), Jan. 14, 2019, 132 Stat. 5538, provided that: ''The amendments made by this subsection [amending this section] shall take effect on the date that is 1 year after the date of the enactment of this Act [Jan. 14, 2019].''

EFFECTIVE DATE OF 2002 AMENDMENT

Amendment by Pub. L. 107–347 effective Dec. 17, 2002, see section 402(b) of Pub. L. 107–347, set out as a note under section 3504 of this title.

Amendment by Pub. L. 107–296 effective 60 days after Nov. 25, 2002, see section 4 of Pub. L. 107–296, set out as an Effective Date note under section 101 of Title 6, Domestic Security.

EFFECTIVE DATE OF 2000 AMENDMENT

Amendment by Pub. L. 106–398 effective 30 days after Oct. 30, 2000, see section 1 [[div. A], title X, § 1065] of Pub. L. 106–398, Oct. 30, 2000, 114 Stat. 1654, formerly set out as an Effective Date note under former section 3531 of this title.

EFFECTIVE DATE OF 1996 AMENDMENT

Amendment by Pub. L. 104–106 effective 180 days after Feb. 10, 1996, see section 5701 of Pub. L. 104–106, Feb. 10, 1996, 110 Stat. 702.

EFFECTIVE DATE

Section effective Oct. 1, 1995, except as otherwise provided, see section 4(a) of Pub. L. 104–13, set out as a note under section 3501 of this title.

USE OF OPEN DATA ASSETS

Pub. L. 115–435, title II, § 202(c)(2), Jan. 14, 2019, 132 Stat. 5538, provided that: ''Not later than 1 year after the date of the enactment of this Act [Jan. 14, 2019], the head of each agency (as defined in section 3502 of title 44, United States Code) shall ensure that any activity by the agency meets the requirements of section 3506 of title 44, United States Code, as amended by this subsection.''

Executive Documents

EX. ORD. NO. 13073. YEAR 2000 CONVERSION

Ex. Ord. No. 13073, Feb. 4, 1998, 63 F.R. 6467, as amended by Ex. Ord. No. 13127, June 14, 1999, 64 F.R. 32793, provided:

The American people expect reliable service from their Government and deserve the confidence that critical government functions dependent on electronic systems will be performed accurately and in a timely manner. Because of a design feature in many electronic systems, a large number of activities in the public and private sectors could be at risk beginning in the year 2000. Some computer systems and other electronic devices will misinterpret the year ''00'' as 1900, rather than 2000. Unless appropriate action is taken, this flaw, known as the ''Y2K problem,'' can cause systems that support those functions to compute erroneously or simply not run. Minimizing the Y2K problem will require a major technological and managerial effort, and it is critical that the United States Government do its part in addressing this challenge.

Accordingly, by the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

SECTION 1. *Policy*. (a) It shall be the policy of the executive branch that agencies shall:

(1) assure that no critical Federal program experiences disruption because of the Y2K problem;

(2) assist and cooperate with State, local, and tribal governments to address the Y2K problem where those governments depend on Federal information or information technology or the Federal Government is dependent on those governments to perform critical missions;

(3) cooperate with the private sector operators of critical national and local systems, including the banking and financial system, the telecommunications system, the public health system, the transportation system, and the electric power generation system, in addressing the Y2K problem; and

(4) communicate with their foreign counterparts to raise awareness of and generate cooperative international arrangements to address the Y2K problem.

(b) As used in this order, ''agency'' and ''agencies'' refer to Federal agencies that are not in the judicial or legislative branches.

SEC. 2. *Year 2000 Conversion Council*. There is hereby established the President's Council on Year 2000 Conversion (the ''Council'').

(a) The Council shall be led by a Chair who shall be an Assistant to the President, and it shall be composed of one representative from each of the executive departments and from such other Federal agencies as may be determined by the Chair of the Council (the ''Chair'').

(b) The Chair shall appoint a Vice Chair and assign other responsibilities for operations of the council as he or she deems necessary.

(c) The Chair shall oversee the activities of agencies to assure that their systems operate smoothly through the year 2000, act as chief spokesperson on this issue for the executive branch in national and international fora, provide policy coordination of executive branch

activities with State, local, and tribal governments on the Y2K problem, and promote appropriate Federal roles with respect to private sector activities in this area.

(d) The Chair and the Director of the Office of Management and Budget shall report jointly at least quarterly to me on the progress of agencies in addressing the Y2K problem.

(e) The Chair shall identify such resources from agencies as the Chair deems necessary for the implementation of the policies set out in this order, consistent with applicable law.

SEC. 3. *Responsibilities of Agency Heads*. (a) The head of each agency shall:

(1) assure that efforts to address the Y2K problem receive the highest priority attention in the agency and that the policies established in this order are carried out; and

(2) cooperate to the fullest extent with the Chair by making available such information, support, and assistance, including personnel, as the Chair may request to support the accomplishment of the tasks assigned herein, consistent with applicable law.

(b) The heads of executive departments and the agencies designated by the Chair under section 2(a) of this order shall identify a responsible official to represent the head of the executive department or agency on the Council with sufficient authority and experience to commit agency resources to address the Y2K problem.

SEC. 4. *Responsibilities of Interagency and Executive Office Councils*. Interagency councils and councils within the Executive Office of the President, including the President's Management Council, the Chief Information Officers Council, the Chief Financial Officers Council, the President's Council on Integrity and Efficiency, the Executive Council on Integrity and Efficiency, the National Science and Technology Council, the National Performance Review, the National Economic Council, the Domestic Policy Council, and the National Security Council shall provide assistance and support to the Chair upon the Chair's request.

SEC. 5. *Information Coordination Center*. (a) To assist the Chair in the Y2K response duties included under section 2(c) of this order, there shall be established the Information Coordination Center (ICC) in the General Services Administration.

(b) At the direction of the Chair, the ICC will assist in making preparations for information sharing and coordination within the Federal Government and key components of the public and private sectors, coordinating agency assessments of Y2K emergencies that could have an adverse affect on U.S. interests at home and abroad, and, if necessary, assisting Federal agencies and the Chair in reconstitution processes where appropriate.

(c) The ICC will:

(1) consist of officials from executive agencies, designated by agency heads under subsection 3(a)(2) of this order, who have expertise in important management and technical areas, computer hardware, software or security systems, reconstitution and recovery, and of additional personnel hired directly or by contract, as required, to carry out the duties described under section 5 of this order;

(2) work with the Council and the Office of Management and Budget to assure that Federal efforts to restore critical systems are coordinated with efforts managed by Federal agencies acting under existing emergency response authorities.

(d) The Chair of the President's Council on Year 2000 Conversion shall designate a Director of the ICC.

SEC. 6. *Judicial Review*. This Executive order is intended only to improve the internal management of the executive branch and does not create any right or benefit, substantive or procedural, enforceable at law or equity by a party against the United States, its agencies, or instrumentalities, its officers or employees, or any other person.

WILLIAM J. CLINTON.

§ 3507. Public information collection activities; submission to Director; approval and delegation

(a) An agency shall not conduct or sponsor the collection of information unless in advance of the adoption or revision of the collection of information—

(1) the agency has—

(A) conducted the review established under section 3506(c)(1);

(B) evaluated the public comments received under section 3506(c)(2);

(C) submitted to the Director the certification required under section 3506(c)(3), the proposed collection of information, copies of pertinent statutory authority, regulations, and other related materials as the Director may specify; and

(D) published a notice in the Federal Register—

(i) stating that the agency has made such submission; and

(ii) setting forth—

(I) a title for the collection of information;

(II) a summary of the collection of information;

(III) a brief description of the need for the information and the proposed use of the information;

(IV) a description of the likely respondents and proposed frequency of response to the collection of information;

(V) an estimate of the burden that shall result from the collection of information; and

(VI) notice that comments may be submitted to the agency and Director;

(2) the Director has approved the proposed collection of information or approval has been inferred, under the provisions of this section; and

(3) the agency has obtained from the Director a control number to be displayed upon the collection of information.

(b) The Director shall provide at least 30 days for public comment prior to making a decision under subsection (c), (d), or (h), except as provided under subsection (j).

(c)(1) For any proposed collection of information not contained in a proposed rule, the Director shall notify the agency involved of the decision to approve or disapprove the proposed collection of information.

(2) The Director shall provide the notification under paragraph (1), within 60 days after receipt or publication of the notice under subsection (a)(1)(D), whichever is later.

(3) If the Director does not notify the agency of a denial or approval within the 60-day period described under paragraph (2)—

(A) the approval may be inferred;

(B) a control number shall be assigned without further delay; and

(C) the agency may collect the information for not more than 1 year.

(d)(1) For any proposed collection of information contained in a proposed rule—

(A) as soon as practicable, but no later than the date of publication of a notice of proposed

rulemaking in the Federal Register, each agency shall forward to the Director a copy of any proposed rule which contains a collection of information and any information requested by the Director necessary to make the determination required under this subsection; and

(B) within 60 days after the notice of proposed rulemaking is published in the Federal Register, the Director may file public comments pursuant to the standards set forth in section 3508 on the collection of information contained in the proposed rule;

(2) When a final rule is published in the Federal Register, the agency shall explain—

(A) how any collection of information contained in the final rule responds to the comments, if any, filed by the Director or the public; or

(B) the reasons such comments were rejected.

(3) If the Director has received notice and failed to comment on an agency rule within 60 days after the notice of proposed rulemaking, the Director may not disapprove any collection of information specifically contained in an agency rule.

(4) No provision in this section shall be construed to prevent the Director, in the Director's discretion—

(A) from disapproving any collection of information which was not specifically required by an agency rule;

(B) from disapproving any collection of information contained in an agency rule, if the agency failed to comply with the requirements of paragraph (1) of this subsection;

(C) from disapproving any collection of information contained in a final agency rule, if the Director finds within 60 days after the publication of the final rule that the agency's response to the Director's comments filed under paragraph (2) of this subsection was unreasonable; or

(D) from disapproving any collection of information contained in a final rule, if—

(i) the Director determines that the agency has substantially modified in the final rule the collection of information contained in the proposed rule; and

(ii) the agency has not given the Director the information required under paragraph (1) with respect to the modified collection of information, at least 60 days before the issuance of the final rule.

(5) This subsection shall apply only when an agency publishes a notice of proposed rulemaking and requests public comments.

(6) The decision by the Director to approve or not act upon a collection of information contained in an agency rule shall not be subject to judicial review.

(e)(1) Any decision by the Director under subsection (c), (d), (h), or (j) to disapprove a collection of information, or to instruct the agency to make substantive or material change to a collection of information, shall be publicly available and include an explanation of the reasons for such decision.

(2) Any written communication between the Administrator of the Office of Information and Regulatory Affairs, or any employee of the Office of Information and Regulatory Affairs, and an agency or person not employed by the Federal Government concerning a proposed collection of information shall be made available to the public.

(3) This subsection shall not require the disclosure of—

(A) any information which is protected at all times by procedures established for information which has been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy; or

(B) any communication relating to a collection of information which is not approved under this subchapter, the disclosure of which could lead to retaliation or discrimination against the communicator.

(f)(1) An independent regulatory agency which is administered by 2 or more members of a commission, board, or similar body, may by majority vote void—

(A) any disapproval by the Director, in whole or in part, of a proposed collection of information of that agency; or

(B) an exercise of authority under subsection (d) of section 3507 concerning that agency.

(2) The agency shall certify each vote to void such disapproval or exercise to the Director, and explain the reasons for such vote. The Director shall without further delay assign a control number to such collection of information, and such vote to void the disapproval or exercise shall be valid for a period of 3 years.

(g) The Director may not approve a collection of information for a period in excess of 3 years.

(h)(1) If an agency decides to seek extension of the Director's approval granted for a currently approved collection of information, the agency shall—

(A) conduct the review established under section 3506(c), including the seeking of comment from the public on the continued need for, and burden imposed by the collection of information; and

(B) after having made a reasonable effort to seek public comment, but no later than 60 days before the expiration date of the control number assigned by the Director for the currently approved collection of information, submit the collection of information for review and approval under this section, which shall include an explanation of how the agency has used the information that it has collected.

(2) If under the provisions of this section, the Director disapproves a collection of information contained in an existing rule, or recommends or instructs the agency to make a substantive or material change to a collection of information contained in an existing rule, the Director shall—

(A) publish an explanation thereof in the Federal Register; and

(B) instruct the agency to undertake a rulemaking within a reasonable time limited to consideration of changes to the collection of information contained in the rule and thereafter to submit the collection of information

for approval or disapproval under this subchapter.

(3) An agency may not make a substantive or material modification to a collection of information after such collection has been approved by the Director, unless the modification has been submitted to the Director for review and approval under this subchapter.

(i)(1) If the Director finds that a senior official of an agency designated under section 3506(a) is sufficiently independent of program responsibility to evaluate fairly whether proposed collections of information should be approved and has sufficient resources to carry out this responsibility effectively, the Director may, by rule in accordance with the notice and comment provisions of chapter 5 of title 5, United States Code, delegate to such official the authority to approve proposed collections of information in specific program areas, for specific purposes, or for all agency purposes.

(2) A delegation by the Director under this section shall not preclude the Director from reviewing individual collections of information if the Director determines that circumstances warrant such a review. The Director shall retain authority to revoke such delegations, both in general and with regard to any specific matter. In acting for the Director, any official to whom approval authority has been delegated under this section shall comply fully with the rules and regulations promulgated by the Director.

(j)(1) The agency head may request the Director to authorize a collection of information, if an agency head determines that—

(A) a collection of information—

(i) is needed prior to the expiration of time periods established under this subchapter; and

(ii) is essential to the mission of the agency; and

(B) the agency cannot reasonably comply with the provisions of this subchapter because—

(i) public harm is reasonably likely to result if normal clearance procedures are followed;

(ii) an unanticipated event has occurred; or

(iii) the use of normal clearance procedures is reasonably likely to prevent or disrupt the collection of information or is reasonably likely to cause a statutory or court ordered deadline to be missed.

(2) The Director shall approve or disapprove any such authorization request within the time requested by the agency head and, if approved, shall assign the collection of information a control number. Any collection of information conducted under this subsection may be conducted without compliance with the provisions of this subchapter for a maximum of 180 days after the date on which the Director received the request to authorize such collection.

(Added Pub. L. 104–13, §2, May 22, 1995, 109 Stat. 176; amended Pub. L. 104–106, div. E, title LVI, §5605(d), Feb. 10, 1996, 110 Stat. 700; Pub. L. 106–398, §1 [[div. A], title X, §1064(b)], Oct. 30, 2000, 114 Stat. 1654, 1654A–275.)

Editorial Notes

PRIOR PROVISIONS

A prior section 3507, added Pub. L. 96–511, §2(a), Dec. 11, 1980, 94 Stat. 2819; amended Pub. L. 99–500, §101(m) [title VIII, §817], Oct. 18, 1986, 100 Stat. 1783–308, 1783–338, and Pub. L. 99–591, §101(m) [title VIII, §817], Oct. 30, 1986, 100 Stat. 3341–308, 3341–338, related to submission to Director of public information collection request for an approval or delegation to a senior official of an agency prior to the general amendment of this chapter by Pub. L. 104–13.

Another prior section 3507, Pub. L. 90–620, Oct. 22, 1968, 82 Stat. 1304, provided for cooperation of agencies in making information available, prior to the general amendment of this chapter by Pub. L. 96–511. See section 3510(a) of this title.

AMENDMENTS

2000—Subsecs. (e)(3)(B), (h), (j). Pub. L. 106–398 substituted ''subchapter'' for ''chapter'' wherever appearing.

1996—Subsec. (j)(2). Pub. L. 104–106 substituted ''180 days'' for ''90 days''.

Statutory Notes and Related Subsidiaries

EFFECTIVE DATE OF 2000 AMENDMENT

Amendment by Pub. L. 106–398 effective 30 days after Oct. 30, 2000, see section 1 [[div. A], title X, §1065] of Pub. L. 106–398, Oct. 30, 2000, 114 Stat. 1654, formerly set out as an Effective Date note under former section 3531 of this title.

EFFECTIVE DATE OF 1996 AMENDMENT

Amendment by Pub. L. 104–106 effective 180 days after Feb. 10, 1996, see section 5701 of Pub. L. 104–106, Feb. 10, 1996, 110 Stat. 702.

EFFECTIVE DATE

Section effective Oct. 1, 1995, except as otherwise provided, see section 4(a) of Pub. L. 104–13, set out as a note under section 3501 of this title.

§3508. Determination of necessity for information; hearing

Before approving a proposed collection of information, the Director shall determine whether the collection of information by the agency is necessary for the proper performance of the functions of the agency, including whether the information shall have practical utility. Before making a determination the Director may give the agency and other interested persons an opportunity to be heard or to submit statements in writing. To the extent, if any, that the Director determines that the collection of information by an agency is unnecessary for any reason, the agency may not engage in the collection of information.

(Added Pub. L. 104–13, §2, May 22, 1995, 109 Stat. 179.)

Editorial Notes

PRIOR PROVISIONS

A prior section 3508, added Pub. L. 96–511, §2(a), Dec. 11, 1980, 94 Stat. 2821, related to determination of whether collection of information is necessary for proper performance of functions of agency prior to the general amendment of this chapter by Pub. L. 104–13.

Another prior section 3508, Pub. L. 90–620, Oct. 22, 1968, 82 Stat. 1304, related to unlawful disclosure of information, penalties, and release of information to other agencies, prior to the general amendment of this

chapter by Pub. L. 96–511. See section 3510(b) of this title.

Statutory Notes and Related Subsidiaries

EFFECTIVE DATE

Section effective Oct. 1, 1995, except as otherwise provided, see section 4(a) of Pub. L. 104–13, set out as a note under section 3501 of this title.

§ 3509. Designation of central collection agency

The Director may designate a central collection agency to obtain information for two or more agencies if the Director determines that the needs of such agencies for information will be adequately served by a single collection agency, and such sharing of data is not inconsistent with applicable law. In such cases the Director shall prescribe (with reference to the collection of information) the duties and functions of the collection agency so designated and of the agencies for which it is to act as agent (including reimbursement for costs). While the designation is in effect, an agency covered by the designation may not obtain for itself information for the agency which is the duty of the collection agency to obtain. The Director may modify the designation from time to time as circumstances require. The authority to designate under this section is subject to the provisions of section 3507(f) of this subchapter.

(Added Pub. L. 104–13, § 2, May 22, 1995, 109 Stat. 180; amended Pub. L. 106–398, § 1 [[div. A], title X, § 1064(b)], Oct. 30, 2000, 114 Stat. 1654, 1654A–275.)

Editorial Notes

PRIOR PROVISIONS

A prior section 3509, added Pub. L. 96–511, § 2(a), Dec. 11, 1980, 94 Stat. 2821, related to designation of central collection agency prior to the general amendment of this chapter by Pub. L. 104–13.

Another prior section 3509, Pub. L. 90–620, Oct. 22, 1968, 82 Stat. 1304, related to plans or forms for collecting information, submission to Director, and his approval, prior to the general amendment of this chapter by Pub. L. 96–511.

AMENDMENTS

2000—Pub. L. 106–398 substituted ''subchapter'' for ''chapter''.

Statutory Notes and Related Subsidiaries

EFFECTIVE DATE OF 2000 AMENDMENT

Amendment by Pub. L. 106–398 effective 30 days after Oct. 30, 2000, see section 1 [[div. A], title X, § 1065] of Pub. L. 106–398, Oct. 30, 2000, 114 Stat. 1654, formerly set out as an Effective Date note under former section 3531 of this title.

EFFECTIVE DATE

Section effective Oct. 1, 1995, except as otherwise provided, see section 4(a) of Pub. L. 104–13, set out as a note under section 3501 of this title.

§ 3510. Cooperation of agencies in making information available

(a) The Director may direct an agency to make available to another agency, or an agency may make available to another agency, information obtained by a collection of information if the disclosure is not inconsistent with applicable law.

(b)(1) If information obtained by an agency is released by that agency to another agency, all the provisions of law (including penalties) that relate to the unlawful disclosure of information apply to the officers and employees of the agency to which information is released to the same extent and in the same manner as the provisions apply to the officers and employees of the agency which originally obtained the information.

(2) The officers and employees of the agency to which the information is released, in addition, shall be subject to the same provisions of law, including penalties, relating to the unlawful disclosure of information as if the information had been collected directly by that agency.

(Added Pub. L. 104–13, § 2, May 22, 1995, 109 Stat. 180.)

Editorial Notes

PRIOR PROVISIONS

A prior section 3510, added Pub. L. 96–511, § 2(a), Dec. 11, 1980, 94 Stat. 2822, related to cooperation of agencies in making information available prior to the general amendment of this chapter by Pub. L. 104–13.

Another prior section 3510, Pub. L. 90–620, Oct. 22, 1968, 82 Stat. 1305, authorized promulgation of rules and regulations, prior to the general amendment of this chapter by Pub. L. 96–511. See section 3516 of this title.

Statutory Notes and Related Subsidiaries

EFFECTIVE DATE

Section effective Oct. 1, 1995, except as otherwise provided, see section 4(a) of Pub. L. 104–13, set out as a note under section 3501 of this title.

§ 3511. Data inventory and Federal data catalogue

(a) COMPREHENSIVE DATA INVENTORY.—

(1) IN GENERAL.—In consultation with the Director and in accordance with the guidance established under paragraph (2), the head of each agency shall, to the maximum extent practicable, develop and maintain a comprehensive data inventory that accounts for all data assets created by, collected by, under the control or direction of, or maintained by the agency. The head of each agency shall ensure that such inventory provides a clear and comprehensive understanding of the data assets in the possession of the agency.

(2) GUIDANCE.—The Director shall establish guidance for agencies to develop and maintain comprehensive data inventories under paragraph (1). Such guidance shall include the following:

(A) A requirement for the head of an agency to include in the comprehensive data inventory metadata on each data asset of the agency, including, to the maximum extent practicable, the following:

(i) A description of the data asset, including all variable names and definitions.

(ii) The name or title of the data asset.

(iii) An indication of whether or not the agency—

(I) has determined or can determine if the data asset is—

(aa) an open Government data asset;

(bb) subject to disclosure or partial disclosure or exempt from disclosure under section 552 of title 5;

(cc) a public data asset eligible for disclosure under subsection (b); or

(dd) a data asset not subject to open format or open license requirements due to existing limitations or restrictions on government distribution of the asset; or

(II) as of the date of such indication, has not made such determination.

(iv) Any determination made under section 3582, if available.

(v) A description of the method by which the public may access or request access to the data asset.

(vi) The date on which the data asset was most recently updated.

(vii) Each agency responsible for maintaining the data asset.

(viii) The owner of the data asset.

(ix) To the extent practicable, any restriction on the use of the data asset.

(x) The location of the data asset.

(xi) Any other metadata necessary to make the comprehensive data inventory useful to the agency and the public, or otherwise determined useful by the Director.

(B) A requirement for the head of an agency to exclude from the comprehensive data inventory any data asset contained on a national security system, as defined in section 11103 of title 40.

(C) Criteria for the head of an agency to use in determining which metadata required by subparagraph (A), if any, in the comprehensive data inventory may not be made publicly available, which shall include, at a minimum, a requirement to ensure all information that could not otherwise be withheld from disclosure under section 552 of title 5 is made public in the comprehensive data inventory.

(D) A requirement for the head of each agency, in accordance with a procedure established by the Director, to submit for inclusion in the Federal data catalogue maintained under subsection (c) the comprehensive data inventory developed pursuant to subparagraph (C), including any real-time updates to such inventory, and data assets made available in accordance with subparagraph (E) or any electronic hyperlink providing access to such data assets.

(E) Criteria for the head of an agency to use in determining whether a particular data asset should not be made publicly available in a manner that takes into account—

(i) risks and restrictions related to the disclosure of personally identifiable information, including the risk that an individual data asset in isolation does not pose a privacy or confidentiality risk but when combined with other available information may pose such a risk;

(ii) security considerations, including the risk that information in an individual data asset in isolation does not pose a security risk but when combined with other available information may pose such a risk;

(iii) the cost and benefits to the public of converting the data into a format that could be understood and used by the public;

(iv) whether the public dissemination of the data asset could result in legal liability;

(v) whether the data asset—

(I) is subject to intellectual property rights, including rights under titles 17 and 35;

(II) contains confidential business information, that could be withheld under section 552(b)(4) of title 5; or

(III) is restricted by contract or other binding, written agreement;

(vi) whether the holder of a right to such data asset has been consulted;

(vii) the expectation that all data assets that would otherwise be made available under section 552 of title 5 be disclosed; and

(viii) any other considerations that the Director determines to be relevant.

(F) Criteria for the head of an agency to use in assessing the indication of a determination under subparagraph (A)(iii) and how to prioritize any such subsequent determinations in the strategic information management plan under section 3506, in consideration of the existing resources available to the agency.

(3) REGULAR UPDATES REQUIRED.—With respect to each data asset created or identified by an agency, the head of the agency shall update the comprehensive data inventory of the agency not later than 90 days after the date of such creation or identification.

(b) PUBLIC DATA ASSETS.—The head of each agency shall submit public data assets, or links to public data assets available online, as open Government data assets for inclusion in the Federal data catalogue maintained under subsection (c), in accordance with the guidance established under subsection (a)(2).

(c) FEDERAL DATA CATALOGUE.—

(1) IN GENERAL.—The Administrator of General Services shall maintain a single public interface online as a point of entry dedicated to sharing agency data assets with the public, which shall be known as the ''Federal data catalogue''. The Administrator and the Director shall ensure that agencies can submit public data assets, or links to public data assets, for publication and public availability on the interface.

(2) REPOSITORY.—The Director shall collaborate with the Office of Government Information Services and the Administrator of General Services to develop and maintain an online repository of tools, best practices, and schema standards to facilitate the adoption of open data practices across the Federal Government, which shall—

(A) include any definitions, regulations, policies, checklists, and case studies related to open data policy;

(B) facilitate collaboration and the adoption of best practices across the Federal

Government relating to the adoption of open data practices; and

(C) be made available on the Federal data catalogue maintained under paragraph (1).

(3) ACCESS TO OTHER DATA ASSETS.—The Director shall ensure the Federal data catalogue maintained under paragraph (1) provides information on how the public can access a data asset included in a comprehensive data inventory under subsection (a) that is not yet available on the Federal data catalogue, including information regarding the application process established under section 3583 of title 44.

(d) DELEGATION.—The Director shall delegate to the Administrator of the Office of Information and Regulatory Affairs and the Administrator of the Office of Electronic Government the authority to jointly issue guidance required under this section.

(Added Pub. L. 104–13, § 2, May 22, 1995, 109 Stat. 180; amended Pub. L. 113–235, div. H, title I, § 1301(c)(1), Dec. 16, 2014, 128 Stat. 2537; Pub. L. 115–435, title II, § 202(d)(1), Jan. 14, 2019, 132 Stat. 5538.)

Editorial Notes

PRIOR PROVISIONS

A prior section 3511, added Pub. L. 96–511, § 2(a), Dec. 11, 1980, 94 Stat. 2822; amended Pub. L. 99–500, § 101(m) [title VIII, § 818], Oct. 18, 1986, 100 Stat. 1783–308, 1783–339, and Pub. L. 99–591, § 101(m) [title VIII, § 818], Oct. 30, 1986, 100 Stat. 3341–308, 3341–339, related to establishment and operation of a Federal Information Locator System prior to the general amendment of this chapter by Pub. L. 104–13.

Another prior section 3511, Pub. L. 90–620, Oct. 22, 1968, 82 Stat. 1305, provided for penalty for failure to furnish information, prior to the general amendment of this chapter by Pub. L. 96–511.

AMENDMENTS

2019—Pub. L. 115–435 amended section generally. Prior to amendment, section related to establishment and operation of Government Information Locator Service.

2014—Subsec. (a)(3). Pub. L. 113–235 substituted ''Director of the Government Publishing Office'' for ''Public Printer''.

Statutory Notes and Related Subsidiaries

EFFECTIVE DATE OF 2019 AMENDMENT

Amendment by Pub. L. 115–435 effective 180 days after Jan. 14, 2019, see section 403 of Pub. L. 115–435, set out as a note under section 306 of Title 5, Government Organization and Employees.

EFFECTIVE DATE

Section effective Oct. 1, 1995, except as otherwise provided, see section 4(a) of Pub. L. 104–13, set out as a note under section 3501 of this title.

§ 3512. Public protection

(a) Notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information that is subject to this subchapter if—

(1) the collection of information does not display a valid control number assigned by the Director in accordance with this subchapter; or

(2) the agency fails to inform the person who is to respond to the collection of information that such person is not required to respond to the collection of information unless it displays a valid control number.

(b) The protection provided by this section may be raised in the form of a complete defense, bar, or otherwise at any time during the agency administrative process or judicial action applicable thereto.

(Added Pub. L. 104–13, § 2, May 22, 1995, 109 Stat. 181; amended Pub. L. 106–398, § 1 [[div. A], title X, § 1064(b)], Oct. 30, 2000, 114 Stat. 1654, 1654A–275.)

Editorial Notes

PRIOR PROVISIONS

A prior section 3512, added Pub. L. 96–511, § 2(a), Dec. 11, 1980, 94 Stat. 2822, related to protection of persons failing to maintain or provide information if information collection request did not display current control number prior to the general amendment of this chapter by Pub. L. 104–13.

Another prior section 3512, added Pub. L. 93–153, title IV, § 409(b), Nov. 16, 1973, 87 Stat. 593, related to information for independent regulatory agencies, prior to the general amendment of this chapter by Pub. L. 96–511.

AMENDMENTS

2000—Subsec. (a). Pub. L. 106–398 substituted ''subchapter'' for ''chapter'' in introductory provisions and par. (1).

Statutory Notes and Related Subsidiaries

EFFECTIVE DATE OF 2000 AMENDMENT

Amendment by Pub. L. 106–398 effective 30 days after Oct. 30, 2000, see section 1 [[div. A], title X, § 1065] of Pub. L. 106–398, Oct. 30, 2000, 114 Stat. 1654, formerly set out as an Effective Date note under former section 3531 of this title.

EFFECTIVE DATE

Section effective Oct. 1, 1995, except as otherwise provided, see section 4(a) of Pub. L. 104–13, set out as a note under section 3501 of this title.

§ 3513. Director review of agency activities; reporting; agency response

(a) In consultation with the Administrator of General Services, the Archivist of the United States, the Director of the National Institute of Standards and Technology, and the Director of the Office of Personnel Management, the Director shall periodically review selected agency information resources management activities to ascertain the efficiency and effectiveness of such activities to improve agency performance and the accomplishment of agency missions.

(b) Each agency having an activity reviewed under subsection (a) shall, within 60 days after receipt of a report on the review, provide a written plan to the Director describing steps (including milestones) to—

(1) be taken to address information resources management problems identified in the report; and

(2) improve agency performance and the accomplishment of agency missions.

(c) COMPARABLE TREATMENT.—Notwithstanding any other provision of law, the Director shall treat or review a rule or order prescribed or proposed by the Director of the Bu-

reau of Consumer Financial Protection on the same terms and conditions as apply to any rule or order prescribed or proposed by the Board of Governors of the Federal Reserve System.

(Added Pub. L. 104–13, § 2, May 22, 1995, 109 Stat. 181; amended Pub. L. 111–203, title X, § 1100D(b), July 21, 2010, 124 Stat. 2111.)

Editorial Notes

PRIOR PROVISIONS

A prior section 3513, added Pub. L. 96–511, § 2(a), Dec. 11, 1980, 94 Stat. 2822; amended Pub. L. 98–497, title I, § 107(b)(27), Oct. 19, 1984, 98 Stat. 2291, related to periodic review of agency activities by Director and report of review and agency response to it prior to the general amendment of this chapter by Pub. L. 104–13.

AMENDMENTS

2010—Subsec. (c). Pub. L. 111–203 added subsec. (c).

Statutory Notes and Related Subsidiaries

EFFECTIVE DATE OF 2010 AMENDMENT

Amendment by Pub. L. 111–203 effective on the designated transfer date, see section 1100H of Pub. L. 111–203, set out as a note under section 552a of Title 5, Government Organization and Employees.

EFFECTIVE DATE

Section effective Oct. 1, 1995, except as otherwise provided, see section 4(a) of Pub. L. 104–13, set out as a note under section 3501 of this title.

§ 3514. Responsiveness to Congress

(a)(1) The Director shall—

(A) keep the Congress and congressional committees fully and currently informed of the major activities under this subchapter; and

(B) submit a report on such activities to the President of the Senate and the Speaker of the House of Representatives annually and at such other times as the Director determines necessary.

(2) The Director shall include in any such report a description of the extent to which agencies have—

(A) reduced information collection burdens on the public, including—

(i) a summary of accomplishments and planned initiatives to reduce collection of information burdens;

(ii) a list of all violations of this subchapter and of any rules, guidelines, policies, and procedures issued pursuant to this subchapter;

(iii) a list of any increase in the collection of information burden, including the authority for each such collection; and

(iv) a list of agencies that in the preceding year did not reduce information collection burdens in accordance with section 3505(a)(1), a list of the programs and statutory responsibilities of those agencies that precluded that reduction, and recommendations to assist those agencies to reduce information collection burdens in accordance with that section;

(B) improved the quality and utility of statistical information;

(C) improved public access to Government information; and

(D) improved program performance and the accomplishment of agency missions through information resources management.

(b) The preparation of any report required by this section shall be based on performance results reported by the agencies and shall not increase the collection of information burden on persons outside the Federal Government.

(Added Pub. L. 104–13, § 2, May 22, 1995, 109 Stat. 181; amended Pub. L. 106–398, § 1 [[div. A], title X, § 1064(b)], Oct. 30, 2000, 114 Stat. 1654, 1654A–275.)

Editorial Notes

PRIOR PROVISIONS

A prior section 3514, added Pub. L. 96–511, § 2(a), Dec. 11, 1980, 94 Stat. 2823, and Pub. L. 99–500, § 101(m) [title VIII, § 819], Oct. 18, 1986, 100 Stat. 1783–308, 1783–339, and Pub. L. 99–591, § 101(m) [title VIII, § 819], Oct. 30, 1986, 100 Stat. 3341–308, 3341–339, related to requirement that Director keep Congress fully informed prior to the general amendment of this chapter by Pub. L. 104–13.

AMENDMENTS

2000—Subsec. (a)(1)(A), (2)(A)(ii). Pub. L. 106–398 substituted ''subchapter'' for ''chapter'' wherever appearing.

Statutory Notes and Related Subsidiaries

EFFECTIVE DATE OF 2000 AMENDMENT

Amendment by Pub. L. 106–398 effective 30 days after Oct. 30, 2000, see section 1 [[div. A], title X, § 1065] of Pub. L. 106–398, Oct. 30, 2000, 114 Stat. 1654, formerly set out as an Effective Date note under former section 3531 of this title.

EFFECTIVE DATE

Section effective Oct. 1, 1995, except as otherwise provided, see section 4(a) of Pub. L. 104–13, set out as a note under section 3501 of this title.

TERMINATION OF REPORTING REQUIREMENTS

For termination, effective May 15, 2000, of provisions of law requiring submittal to Congress of any annual, semiannual, or other regular periodic report listed in House Document No. 103–7 (in which the 8th item on page 41 identifies an annual reporting requirement which, as subsequently amended, is contained in subsec. (a) of this section), see section 3003 of Pub. L. 104–66, as amended, set out as a note under section 1113 of Title 31, Money and Finance.

§ 3515. Administrative powers

Upon the request of the Director, each agency (other than an independent regulatory agency) shall, to the extent practicable, make its services, personnel, and facilities available to the Director for the performance of functions under this subchapter.

(Added Pub. L. 104–13, § 2, May 22, 1995, 109 Stat. 182; amended Pub. L. 106–398, § 1 [[div. A], title X, § 1064(b)], Oct. 30, 2000, 114 Stat. 1654, 1654A–275.)

Editorial Notes

PRIOR PROVISIONS

A prior section 3515, added Pub. L. 96–511, § 2(a), Dec. 11, 1980, 94 Stat. 2824, related to availability of agency services, personnel, and facilities prior to the general amendment of this chapter by Pub. L. 104–13.

AMENDMENTS

2000—Pub. L. 106–398 substituted ''subchapter'' for ''chapter''.

Statutory Notes and Related Subsidiaries

EFFECTIVE DATE OF 2000 AMENDMENT

Amendment by Pub. L. 106–398 effective 30 days after Oct. 30, 2000, see section 1 [[div. A], title X, §1065] of Pub. L. 106–398, Oct. 30, 2000, 114 Stat. 1654, formerly set out as an Effective Date note under former section 3531 of this title.

EFFECTIVE DATE

Section effective Oct. 1, 1995, except as otherwise provided, see section 4(a) of Pub. L. 104–13, set out as a note under section 3501 of this title.

§ 3516. Rules and regulations

The Director shall promulgate rules, regulations, or procedures necessary to exercise the authority provided by this subchapter.

(Added Pub. L. 104–13, §2, May 22, 1995, 109 Stat. 182; amended Pub. L. 106–398, §1 [[div. A], title X, §1064(b)], Oct. 30, 2000, 114 Stat. 1654, 1654A–275.)

Editorial Notes

PRIOR PROVISIONS

A prior section 3516, added Pub. L. 96–511, §2(a), Dec. 11, 1980, 94 Stat. 2824, related to rules and regulations prior to the general amendment of this chapter by Pub. L. 104–13.

AMENDMENTS

2000—Pub. L. 106–398 substituted ''subchapter'' for ''chapter''.

Statutory Notes and Related Subsidiaries

EFFECTIVE DATE OF 2000 AMENDMENT

Amendment by Pub. L. 106–398 effective 30 days after Oct. 30, 2000, see section 1 [[div. A], title X, §1065] of Pub. L. 106–398, Oct. 30, 2000, 114 Stat. 1654, formerly set out as an Effective Date note under former section 3531 of this title.

EFFECTIVE DATE

Section effective Oct. 1, 1995, except as otherwise provided, see section 4(a) of Pub. L. 104–13, set out as a note under section 3501 of this title.

POLICY AND PROCEDURAL GUIDELINES

Pub. L. 106–554, §1(a)(3) [title V, §515], Dec. 21, 2000, 114 Stat. 2763, 2763A–153, provided that:

''(a) IN GENERAL.—The Director of the Office of Management and Budget shall, by not later than September 30, 2001, and with public and Federal agency involvement, issue guidelines under sections 3504(d)(1) and 3516 of title 44, United States Code, that provide policy and procedural guidance to Federal agencies for ensuring and maximizing the quality, objectivity, utility, and integrity of information (including statistical information) disseminated by Federal agencies in fulfillment of the purposes and provisions of chapter 35 of title 44, United States Code, commonly referred to as the Paperwork Reduction Act.

''(b) CONTENT OF GUIDELINES.—The guidelines under subsection (a) shall—

''(1) apply to the sharing by Federal agencies of, and access to, information disseminated by Federal agencies; and

''(2) require that each Federal agency to which the guidelines apply—

''(A) issue guidelines ensuring and maximizing the quality, objectivity, utility, and integrity of information (including statistical information) disseminated by the agency, by not later than 1 year after the date of issuance of the guidelines under subsection (a);

''(B) establish administrative mechanisms allowing affected persons to seek and obtain correction of information maintained and disseminated by the agency that does not comply with the guidelines issued under subsection (a); and

''(C) report periodically to the Director—

''(i) the number and nature of complaints received by the agency regarding the accuracy of information disseminated by the agency; and

''(ii) how such complaints were handled by the agency.''

§ 3517. Consultation with other agencies and the public

(a) In developing information resources management policies, plans, rules, regulations, procedures, and guidelines and in reviewing collections of information, the Director shall provide interested agencies and persons early and meaningful opportunity to comment.

(b) Any person may request the Director to review any collection of information conducted by or for an agency to determine, if, under this subchapter, a person shall maintain, provide, or disclose the information to or for the agency. Unless the request is frivolous, the Director shall, in coordination with the agency responsible for the collection of information—

(1) respond to the request within 60 days after receiving the request, unless such period is extended by the Director to a specified date and the person making the request is given notice of such extension; and

(2) take appropriate remedial action, if necessary.

(Added Pub. L. 104–13, §2, May 22, 1995, 109 Stat. 182; amended Pub. L. 106–398, §1 [[div. A], title X, §1064(b)], Oct. 30, 2000, 114 Stat. 1654, 1654A–275.)

Editorial Notes

PRIOR PROVISIONS

A prior section 3517, added Pub. L. 96–511, §2(a), Dec. 11, 1980, 94 Stat. 2824, related to consultation with other agencies and the public prior to the general amendment of this chapter by Pub. L. 104–13.

AMENDMENTS

2000—Subsec. (b). Pub. L. 106–398 substituted ''subchapter'' for ''chapter'' in introductory provisions.

Statutory Notes and Related Subsidiaries

EFFECTIVE DATE OF 2000 AMENDMENT

Amendment by Pub. L. 106–398 effective 30 days after Oct. 30, 2000, see section 1 [[div. A], title X, §1065] of Pub. L. 106–398, Oct. 30, 2000, 114 Stat. 1654, formerly set out as an Effective Date note under former section 3531 of this title.

EFFECTIVE DATE

Section effective Oct. 1, 1995, except as otherwise provided, see section 4(a) of Pub. L. 104–13, set out as a note under section 3501 of this title.

§ 3518. Effect on existing laws and regulations

(a) Except as otherwise provided in this subchapter, the authority of an agency under any other law to prescribe policies, rules, regula-

tions, and procedures for Federal information resources management activities is subject to the authority of the Director under this subchapter.

(b) Nothing in this subchapter shall be deemed to affect or reduce the authority of the Secretary of Commerce or the Director of the Office of Management and Budget pursuant to Reorganization Plan No. 1 of 1977 (as amended) and Executive order, relating to telecommunications and information policy, procurement and management of telecommunications and information systems, spectrum use, and related matters.

(c)(1) Except as provided in paragraph (2), this subchapter shall not apply to the collection of information—

(A) during the conduct of a Federal criminal investigation or prosecution, or during the disposition of a particular criminal matter;

(B) during the conduct of—

(i) a civil action to which the United States or any official or agency thereof is a party; or

(ii) an administrative action or investigation involving an agency against specific individuals or entities;

(C) by compulsory process pursuant to the Antitrust Civil Process Act and section 13 of the Federal Trade Commission Improvements Act of 1980; or

(D) during the conduct of intelligence activities as defined in section 3.4(e) of Executive Order No. 12333, issued December 4, 1981, or successor orders, or during the conduct of cryptologic activities that are communications security activities.

(2) This subchapter applies to the collection of information during the conduct of general investigations (other than information collected in an antitrust investigation to the extent provided in subparagraph (C) of paragraph (1)) undertaken with reference to a category of individuals or entities such as a class of licensees or an entire industry.

(d) Nothing in this subchapter shall be interpreted as increasing or decreasing the authority conferred by sections 11331 and 11332[1] of title 40 on the Secretary of Commerce or the Director of the Office of Management and Budget.

(e) Nothing in this subchapter shall be interpreted as increasing or decreasing the authority of the President, the Office of Management and Budget or the Director thereof, under the laws of the United States, with respect to the substantive policies and programs of departments, agencies and offices, including the substantive authority of any Federal agency to enforce the civil rights laws.

(Added Pub. L. 104–13, §2, May 22, 1995, 109 Stat. 183; amended Pub. L. 104–106, div. E, title LI, §5131(e)(2), Feb. 10, 1996, 110 Stat. 688; Pub. L. 105–85, div. A, title X, §1073(h)(5)(C), Nov. 18, 1997, 111 Stat. 1907; Pub. L. 106–398, §1 [[div. A], title X, §1064(b)], Oct. 30, 2000, 114 Stat. 1654, 1654A–275; Pub. L. 107–217, §3(*l*)(7), Aug. 21, 2002, 116 Stat. 1302.)

[1] See References in Text note below.

Editorial Notes

REFERENCES IN TEXT

Reorganization Plan No. 1 of 1977, referred to in subsec. (b), is set out in the Appendix to Title 5, Government Organization and Employees.

Executive order, referred to in subsec. (b), probably means Ex. Ord. No. 12046, Mar. 27, 1978, 43 F.R. 13349, which is set out as a note under section 305 of Title 47, Telecommunications.

The Antitrust Civil Process Act, referred to in subsec. (c)(1)(C), is Pub. L. 87–664, Sept. 19, 1962, 76 Stat. 548, which is classified principally to chapter 34 (§1311 et seq.) of Title 15, Commerce and Trade. For complete classification of this Act to the Code, see Short Title note set out under section 1311 of Title 15 and Tables.

Section 13 of the Federal Trade Commission Improvements Act of 1980, referred to in subsec. (c)(1)(C), is classified to section 57b–1 of Title 15.

Executive Order No. 12333, referred to in subsec. (c)(1)(D), is Ex. Ord. No. 12333, Dec. 4, 1981, 46 F.R. 59941, which is set out as a note under section 3001 of Title 50, War and National Defense.

Section 11332 of title 40, referred to in subsec. (d), was repealed by Pub. L. 107–296, title X, §1005(a)(1), Nov. 25, 2002, 116 Stat. 2272, and Pub. L. 107–347, title III, §305(a), Dec. 17, 2002, 116 Stat. 2960.

PRIOR PROVISIONS

A prior section 3518, added Pub. L. 96–511, §2(a), Dec. 11, 1980, 94 Stat. 2824, related to the effect on existing laws and regulations prior to the general amendment of this chapter by Pub. L. 104–13.

AMENDMENTS

2002—Subsec. (d). Pub. L. 107–217 substituted ''sections 11331 and 11332 of title 40'' for ''section 5131 of the Clinger-Cohen Act of 1996 (40 U.S.C. 1441) and the Computer Security Act of 1987 (40 U.S.C. 759 note)''.

2000—Pub. L. 106–398 substituted ''subchapter'' for ''chapter'' wherever appearing.

1997—Subsec. (d). Pub. L. 105–85 substituted ''Clinger-Cohen Act of 1996 (40 U.S.C. 1441)'' for ''Information Technology Management Reform Act of 1996''.

1996—Subsec. (d). Pub. L. 104–106 substituted ''section 5131 of the Information Technology Management Reform Act of 1996 and the Computer Security Act of 1987 (40 U.S.C. 759 note) on the Secretary of Commerce or'' for ''Public Law 89–306 on the Administrator of the General Services Administration, the Secretary of Commerce, or''.

Statutory Notes and Related Subsidiaries

EFFECTIVE DATE OF 2000 AMENDMENT

Amendment by Pub. L. 106–398 effective 30 days after Oct. 30, 2000, see section 1 [[div. A], title X, §1065] of Pub. L. 106–398, Oct. 30, 2000, 114 Stat. 1654, formerly set out as an Effective Date note under former section 3531 of this title.

EFFECTIVE DATE OF 1996 AMENDMENT

Amendment by Pub. L. 104–106 effective 180 days after Feb. 10, 1996, see section 5701 of Pub. L. 104–106, Feb. 10, 1996, 110 Stat. 702.

EFFECTIVE DATE

Section effective Oct. 1, 1995, except as otherwise provided, see section 4(a) of Pub. L. 104–13, set out as a note under section 3501 of this title.

§3519. Access to information

Under the conditions and procedures prescribed in section 716 of title 31, the Director and personnel in the Office of Information and Regulatory Affairs shall furnish such information as the Comptroller General may require for the dis-

charge of the responsibilities of the Comptroller General. For the purpose of obtaining such information, the Comptroller General or representatives thereof shall have access to all books, documents, papers and records, regardless of form or format, of the Office.

(Added Pub. L. 104–13, § 2, May 22, 1995, 109 Stat. 183.)

Editorial Notes

PRIOR PROVISIONS

A prior section 3519, added Pub. L. 96–511, § 2(a), Dec. 11, 1980, 94 Stat. 2825; amended Pub. L. 97–258, § 3(m)(3), Sept. 13, 1982, 96 Stat. 1066, related to access to information prior to the general amendment of this chapter by Pub. L. 104–13.

Statutory Notes and Related Subsidiaries

EFFECTIVE DATE

Section effective Oct. 1, 1995, except as otherwise provided, see section 4(a) of Pub. L. 104–13, set out as a note under section 3501 of this title.

§ 3520. Chief Data Officers

(a) ESTABLISHMENT.—The head of each agency shall designate a nonpolitical appointee employee in the agency as the Chief Data Officer of the agency.

(b) QUALIFICATIONS.—The Chief Data Officer of an agency shall be designated on the basis of demonstrated training and experience in data management, governance (including creation, application, and maintenance of data standards), collection, analysis, protection, use, and dissemination, including with respect to any statistical and related techniques to protect and de-identify confidential data.

(c) FUNCTIONS.—The Chief Data Officer of an agency shall—

(1) be responsible for lifecycle data management;

(2) coordinate with any official in the agency responsible for using, protecting, disseminating, and generating data to ensure that the data needs of the agency are met;

(3) manage data assets of the agency, including the standardization of data format, sharing of data assets, and publication of data assets in accordance with applicable law;

(4) in carrying out the requirements under paragraphs (3) and (5), consult with any statistical official of the agency (as designated under section 314 of title 5);

(5) carry out the requirements of the agency under subsections (b) through (d), (f), and (i) of section 3506, section 3507, and section 3511;

(6) ensure that, to the extent practicable, agency data conforms with data management best practices;

(7) engage agency employees, the public, and contractors in using public data assets and encourage collaborative approaches on improving data use;

(8) support the Performance Improvement Officer of the agency in identifying and using data to carry out the functions described in section 1124(a)(2) of title 31;

(9) support the Evaluation Officer of the agency in obtaining data to carry out the functions described in section 313(d) of title 5;

(10) review the impact of the infrastructure of the agency on data asset accessibility and coordinate with the Chief Information Officer of the agency to improve such infrastructure to reduce barriers that inhibit data asset accessibility;

(11) ensure that, to the extent practicable, the agency maximizes the use of data in the agency, including for the production of evidence (as defined in section 3561), cybersecurity, and the improvement of agency operations;

(12) identify points of contact for roles and responsibilities related to open data use and implementation (as required by the Director);

(13) serve as the agency liaison to other agencies and the Office of Management and Budget on the best way to use existing agency data for statistical purposes (as defined in section 3561); and

(14) comply with any regulation and guidance issued under subchapter III, including the acquisition and maintenance of any required certification and training.

(d) DELEGATION OF RESPONSIBILITIES.—

(1) IN GENERAL.—To the extent necessary to comply with statistical laws, the Chief Data Officer of an agency shall delegate any responsibility under subsection (c) to the head of a statistical agency or unit (as defined in section 3561) within the agency.

(2) CONSULTATION.—To the extent permissible under law, the individual to whom a responsibility has been delegated under paragraph (1) shall consult with the Chief Data Officer of the agency in carrying out such responsibility.

(3) DEFERENCE.—The Chief Data Officer of the agency shall defer to the individual to whom a responsibility has been delegated under paragraph (1) regarding the necessary delegation of such responsibility with respect to any data acquired, maintained, or disseminated by the agency under applicable statistical law.

(e) REPORTS.—The Chief Data Officer of an agency shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Oversight and Government Reform of the House of Representatives an annual report on the compliance of the agency with the requirements of this subchapter, including information on each requirement that the agency could not carry out and, if applicable, what the agency needs to carry out such requirement.

(Added Pub. L. 107–198, § 3(a)(2), June 28, 2002, 116 Stat. 730; amended Pub. L. 115–435, title II, § 202(e)(1), Jan. 14, 2019, 132 Stat. 5541.)

Editorial Notes

PRIOR PROVISIONS

A prior section 3520 was renumbered section 3521 of this title.

Another prior section 3520, added Pub. L. 96–511, § 2(a), Dec. 11, 1980, 94 Stat. 2825; amended Pub. L. 99–500, § 101(m) [title VIII, § 820], Oct. 18, 1986, 100 Stat. 1783–308, 1783–340, and Pub. L. 99–591, § 101(m) [title VIII, § 820], Oct. 30, 1986, 100 Stat. 3341–308, 3341–340, related to au-

thorization of appropriations prior to the general amendment of this chapter by Pub. L. 104–13.

AMENDMENTS

2019—Pub. L. 115–435 amended section generally. Prior to amendment, section related to establishment of task force on information collection and dissemination.

Statutory Notes and Related Subsidiaries

CHANGE OF NAME

Committee on Oversight and Government Reform of House of Representatives changed to Committee on Oversight and Reform of House of Representatives by House Resolution No. 6, One Hundred Sixteenth Congress, Jan. 9, 2019. Committee on Oversight and Reform of House of Representatives changed to Committee on Oversight and Accountability of House of Representatives by House Resolution No. 5, One Hundred Eighteenth Congress, Jan. 9, 2023.

EFFECTIVE DATE OF 2019 AMENDMENT

Amendment by Pub. L. 115–435 effective 180 days after Jan. 14, 2019, see section 403 of Pub. L. 115–435, set out as a note under section 306 of Title 5, Government Organization and Employees.

§ 3520A. Chief Data Officer Council

(a) ESTABLISHMENT.—There is established in the Office of Management and Budget a Chief Data Officer Council (in this section referred to as the ''Council'').

(b) PURPOSE AND FUNCTIONS.—The Council shall—

(1) establish Governmentwide best practices for the use, protection, dissemination, and generation of data;

(2) promote and encourage data sharing agreements between agencies;

(3) identify ways in which agencies can improve upon the production of evidence for use in policymaking;

(4) consult with the public and engage with private users of Government data and other stakeholders on how to improve access to data assets of the Federal Government; and

(5) identify and evaluate new technology solutions for improving the collection and use of data.

(c) MEMBERSHIP.—

(1) IN GENERAL.—The Chief Data Officer of each agency shall serve as a member of the Council.

(2) CHAIR.—The Director shall select the Chair of the Council from among the members of the Council.

(3) ADDITIONAL MEMBERS.—The Administrator of the Office of Electronic Government shall serve as a member of the Council.

(4) EX OFFICIO MEMBER.—The Director shall appoint a representative for all Chief Information Officers and Evaluation Officers, and such representative shall serve as an ex officio member of the Council.

(d) REPORTS.—The Council shall submit to the Director, the Committee on Homeland Security and Governmental Affairs of the Senate, and the Committee on Oversight and Government Reform of the House of Representatives a biennial report on the work of the Council.

(e) EVALUATION AND TERMINATION.—

(1) GAO EVALUATION OF COUNCIL.—Not later than 4 years after date[1] of the enactment of this section, the Comptroller General shall submit to Congress a report on whether the additional duties of the Council improved the use of evidence and program evaluation in the Federal Government.

(2) TERMINATION OF COUNCIL.—The Council shall terminate and this section shall be repealed upon the expiration of the 2-year period that begins on the date the Comptroller General submits the report under paragraph (1) to Congress.

(Added Pub. L. 115–435, title II, § 202(f)(1), Jan. 14, 2019, 132 Stat. 5542.)

Editorial Notes

REFERENCES IN TEXT

The date of the enactment of this section, referred to in subsec. (e)(1), is the date of enactment of Pub. L. 115–435, which was approved Jan. 14, 2019.

Statutory Notes and Related Subsidiaries

CHANGE OF NAME

Committee on Oversight and Government Reform of House of Representatives changed to Committee on Oversight and Reform of House of Representatives by House Resolution No. 6, One Hundred Sixteenth Congress, Jan. 9, 2019. Committee on Oversight and Reform of House of Representatives changed to Committee on Oversight and Accountability of House of Representatives by House Resolution No. 5, One Hundred Eighteenth Congress, Jan. 9, 2023.

EFFECTIVE DATE

Section effective 180 days after Jan. 14, 2019, see section 403 of Pub. L. 115–435, set out as an Effective Date of 2019 Amendment note under section 306 of Title 5, Government Organization and Employees.

§ 3521. Authorization of appropriations

There are authorized to be appropriated to the Office of Information and Regulatory Affairs to carry out the provisions of this subchapter, and for no other purpose, $8,000,000 for each of the fiscal years 1996, 1997, 1998, 1999, 2000, and 2001.

(Added Pub. L. 104–13, § 2, May 22, 1995, 109 Stat. 184, § 3520; amended Pub. L. 106–398, § 1 [[div. A], title X, § 1064(b)], Oct. 30, 2000, 114 Stat. 1654, 1654A–275; renumbered § 3521, Pub. L. 107–198, § 3(a)(1), June 28, 2002, 116 Stat. 730.)

Editorial Notes

AMENDMENTS

2002—Pub. L. 107–198 renumbered section 3520 of this title as this section.

2000—Pub. L. 106–398 substituted ''subchapter'' for ''chapter''.

Statutory Notes and Related Subsidiaries

EFFECTIVE DATE OF 2000 AMENDMENT

Amendment by Pub. L. 106–398 effective 30 days after Oct. 30, 2000, see section 1 [[div. A], title X, § 1065] of Pub. L. 106–398, Oct. 30, 2000, 114 Stat. 1654, formerly set out as an Effective Date note under former section 3531 of this title.

[1] So in original. Probably should be preceded by ''the''.

EFFECTIVE DATE

Section effective May 22, 1995, see section 4 of Pub. L. 104–13, set out as a note under section 3501 of this title.

[§§ 3531 to 3549. Repealed. Pub. L. 113–283, § 2(a), Dec. 18, 2014, 128 Stat. 3073]

Sections 3531 to 3538 comprised subchapter II of this chapter ''INFORMATION SECURITY''.

Section 3531, added Pub. L. 107–296, title X, § 1001(b)(1), Nov. 25, 2002, 116 Stat. 2259, set forth purposes of subchapter II. See section 3551 of this title.

A prior section 3531, added Pub. L. 106–398, § 1 [[div. A], title X, § 1061], Oct. 30, 2000, 114 Stat. 1654, 1654A–266, set forth purposes of subchapter II prior to the general amendment of subchapter II by Pub. L. 107–296.

Section 3532, added Pub. L. 107–296, title X, § 1001(b)(1), Nov. 25, 2002, 116 Stat. 2260, related to definitions applicable to subchapter II. See section 3552 of this title.

A prior section 3532, added Pub. L. 106–398, § 1 [[div. A], title X, § 1061], Oct. 30, 2000, 114 Stat. 1654, 1654A–266, related to definitions applicable to subchapter II prior to the general amendment of subchapter II by Pub. L. 107–296.

Section 3533, added Pub. L. 107–296, title X, § 1001(b)(1), Nov. 25, 2002, 116 Stat. 2261, set forth authority and functions of the Director. See section 3553 of this title.

A prior section 3533, added Pub. L. 106–398, § 1 [[div. A], title X, § 1061], Oct. 30, 2000, 114 Stat. 1654, 1654A–266, set forth authority and functions of the Director prior to the general amendment of subchapter II by Pub. L. 107–296.

Section 3534, added Pub. L. 107–296, title X, § 1001(b)(1), Nov. 25, 2002, 116 Stat. 2262, related to Federal agency responsibilities. See section 3554 of this title.

A prior section 3534, added Pub. L. 106–398, § 1 [[div. A], title X, § 1061], Oct. 30, 2000, 114 Stat. 1654, 1654A–268, related to Federal agency responsibilities prior to the general amendment of subchapter II by Pub. L. 107–296.

Section 3535, added Pub. L. 107–296, title X, § 1001(b)(1), Nov. 25, 2002, 116 Stat. 2265; amended Pub. L. 108–177, title III, § 377(e), Dec. 13, 2003, 117 Stat. 2631, related to annual independent evaluation. See section 3555 of this title.

A prior section 3535, added Pub. L. 106–398, § 1 [[div. A], title X, § 1061], Oct. 30, 2000, 114 Stat. 1654, 1654A–271, related to annual independent evaluation prior to the general amendment of subchapter II by Pub. L. 107–296.

Section 3536, added Pub. L. 107–296, title X, § 1001(b)(1), Nov. 25, 2002, 116 Stat. 2266, described responsibilities for the head of each agency operating or exercising control of a national security system. See section 3557 of this title.

A prior section 3536, added Pub. L. 106–398, § 1 [[div. A], title X, § 1061], Oct. 30, 2000, 114 Stat. 1654, 1654A–272; amended Pub. L. 107–314, div. A, title X, § 1052(a), Dec. 2, 2002, 116 Stat. 2648, set forth expiration date of subchapter II prior to the general amendment of subchapter II by Pub. L. 107–296.

Section 3537, added Pub. L. 107–296, title X, § 1001(b)(1), Nov. 25, 2002, 116 Stat. 2267, authorized appropriations for fiscal years 2003 through 2007.

Section 3538, added Pub. L. 107–296, title X, § 1001(b)(1), Nov. 25, 2002, 116 Stat. 2267, related to effect on existing law. See section 3558 of this title.

Sections 3541 to 3549 comprised subchapter III of this chapter ''INFORMATION SECURITY''.

Section 3541, added Pub. L. 107–347, title III, § 301(b)(1), Dec. 17, 2002, 116 Stat. 2946, set forth purposes of subchapter III. See section 3551 of this title.

Section 3542, added Pub. L. 107–347, title III, § 301(b)(1), Dec. 17, 2002, 116 Stat. 2947, related to definitions applicable to subchapter III. See section 3552 of this title.

Section 3543, added Pub. L. 107–347, title III, § 301(b)(1), Dec. 17, 2002, 116 Stat. 2947, set forth authority and functions of the Director. See section 3553 of this title.

Section 3544, added Pub. L. 107–347, title III, § 301(b)(1), Dec. 17, 2002, 116 Stat. 2949, related to Federal agency responsibilities. See section 3554 of this title.

Section 3545, added Pub. L. 107–347, title III, § 301(b)(1), Dec. 17, 2002, 116 Stat. 2952; amended Pub. L. 108–177, title III, § 377(e), Dec. 13, 2003, 117 Stat. 2631, related to annual independent evaluation. See section 3555 of this title.

Section 3546, added Pub. L. 107–347, title III, § 301(b)(1), Dec. 17, 2002, 116 Stat. 2954, related to Federal information security incident center. See section 3556 of this title.

Section 3547, added Pub. L. 107–347, title III, § 301(b)(1), Dec. 17, 2002, 116 Stat. 2954, described responsibilities for the head of each agency operating or exercising control of a national security system. See section 3557 of this title.

Section 3548, added Pub. L. 107–347, title III, § 301(b)(1), Dec. 17, 2002, 116 Stat. 2954, authorized appropriations for fiscal years 2003 through 2007.

Section 3549, added Pub. L. 107–347, title III, § 301(b)(1), Dec. 17, 2002, 116 Stat. 2955, related to effect on existing law and provided that subchapter II was not to apply while subchapter III was in effect. See section 3558 of this title.

SUBCHAPTER II—INFORMATION SECURITY

§ 3551. Purposes

The purposes of this subchapter are to—

(1) provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets;

(2) recognize the highly networked nature of the current Federal computing environment and provide effective governmentwide management and oversight of the related information security risks, including coordination of information security efforts throughout the civilian, national security, and law enforcement communities;

(3) provide for development and maintenance of minimum controls required to protect Federal information and information systems;

(4) provide a mechanism for improved oversight of Federal agency information security programs, including through automated security tools to continuously diagnose and improve security;

(5) acknowledge that commercially developed information security products offer advanced, dynamic, robust, and effective information security solutions, reflecting market solutions for the protection of critical information infrastructures important to the national defense and economic security of the nation that are designed, built, and operated by the private sector; and

(6) recognize that the selection of specific technical hardware and software information security solutions should be left to individual agencies from among commercially developed products.

(Added Pub. L. 113–283, § 2(a), Dec. 18, 2014, 128 Stat. 3073.)

Editorial Notes

PRIOR PROVISIONS

Provisions similar to this section were contained in sections 3531 and 3541 of this title prior to repeal by Pub. L. 113–283.

Statutory Notes and Related Subsidiaries

CYBERSECURITY IMPROVEMENTS TO AGENCY INFORMATION SYSTEMS

Pub. L. 114–4, title V, § 547, Mar. 4, 2015, 129 Stat. 69, provided that:

''(a) Of the amounts made available by this Act [Pub. L. 114–4, see Tables for classification] for 'National Protection and Programs Directorate, Infrastructure Protection and Information Security', $140,525,000 for the Federal Network Security program, project, and activity shall be used to deploy on Federal systems technology to improve the information security of agency information systems covered by [former] section 3543(a) of title 44, United States Code [see now 44 U.S.C. 3553]: *Provided*, That funds made available under this section shall be used to assist and support Government-wide and agency-specific efforts to provide adequate, risk-based, and cost-effective cybersecurity to address escalating and rapidly evolving threats to information security, including the acquisition and operation of a continuous monitoring and diagnostics program, in collaboration with departments and agencies, that includes equipment, software, and Department of Homeland Security supplied services: *Provided further*, That continuous monitoring and diagnostics software procured by the funds made available by this section shall not transmit to the Department of Homeland Security any personally identifiable information or content of network communications of other agencies' users: *Provided further*, That such software shall be installed, maintained, and operated in accordance with all applicable privacy laws and agency-specific policies regarding network content.

''(b) Funds made available under this section may not be used to supplant funds provided for any such system within an agency budget.

''(c) Not later than July 1, 2015, the heads of all Federal agencies shall submit to the Committees on Appropriations of the Senate and the House of Representatives expenditure plans for necessary cybersecurity improvements to address known vulnerabilities to information systems described in subsection (a).

''(d) Not later than October 1, 2015, and semiannually thereafter, the head of each Federal agency shall submit to the Director of the Office of Management and Budget a report on the execution of the expenditure plan for that agency required by subsection (c): *Provided*, That the Director of the Office of Management and Budget shall summarize such execution reports and annually submit such summaries to Congress in conjunction with the annual progress report on implementation of the E-Government Act of 2002 (Public Law 107–347) [see Tables for classification], as required by section 3606 of title 44, United States Code.

''(e) This section shall not apply to the legislative and judicial branches of the Federal Government and shall apply to all Federal agencies within the executive branch except for the Department of Defense, the Central Intelligence Agency, and the Office of the Director of National Intelligence.''

Similar provisions were contained in the following prior appropriation acts:

Pub. L. 113–76, div. F, title V, § 554, Jan. 17, 2014, 128 Stat. 278.

Pub. L. 113–6, div. D, title V, § 558, Mar. 26, 2013, 127 Stat. 377.

Executive Documents

EX. ORD. NO. 14028. IMPROVING THE NATION'S CYBERSECURITY

Ex. Ord. No. 14028, May 12, 2021, 86 F.R. 26633, provided:

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

SECTION 1. *Policy*. The United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people's security and privacy. The Federal Government must improve its efforts to identify, deter, protect against, detect, and respond to these actions and actors. The Federal Government must also carefully examine what occurred during any major cyber incident and apply lessons learned. But cybersecurity requires more than government action. Protecting our Nation from malicious cyber actors requires the Federal Government to partner with the private sector. The private sector must adapt to the continuously changing threat environment, ensure its products are built and operate securely, and partner with the Federal Government to foster a more secure cyberspace. In the end, the trust we place in our digital infrastructure should be proportional to how trustworthy and transparent that infrastructure is, and to the consequences we will incur if that trust is misplaced.

Incremental improvements will not give us the security we need; instead, the Federal Government needs to make bold changes and significant investments in order to defend the vital institutions that underpin the American way of life. The Federal Government must bring to bear the full scope of its authorities and resources to protect and secure its computer systems, whether they are cloud-based, on-premises, or hybrid. The scope of protection and security must include systems that process data (information technology (IT)) and those that run the vital machinery that ensures our safety (operational technology (OT)).

It is the policy of my Administration that the prevention, detection, assessment, and remediation of cyber incidents is a top priority and essential to national and economic security. The Federal Government must lead by example. All Federal Information Systems should meet or exceed the standards and requirements for cybersecurity set forth in and issued pursuant to this order.

SEC. 2. *Removing Barriers to Sharing Threat Information*. (a) The Federal Government contracts with IT and OT service providers to conduct an array of day-to-day functions on Federal Information Systems. These service providers, including cloud service providers, have unique access to and insight into cyber threat and incident information on Federal Information Systems. At the same time, current contract terms or restrictions may limit the sharing of such threat or incident information with executive departments and agencies (agencies) that are responsible for investigating or remediating cyber incidents, such as the Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and other elements of the Intelligence Community (IC). Removing these contractual barriers and increasing the sharing of information about such threats, incidents, and risks are necessary steps to accelerating incident deterrence, prevention, and response efforts and to enabling more effective defense of agencies' systems and of information collected, processed, and maintained by or for the Federal Government.

(b) Within 60 days of the date of this order [May 12, 2021], the Director of the Office of Management and Budget (OMB), in consultation with the Secretary of Defense, the Attorney General, the Secretary of Homeland Security, and the Director of National Intelligence, shall review the Federal Acquisition Regulation (FAR) and the Defense Federal Acquisition Regulation Supplement contract requirements and language for contracting with IT and OT service providers and recommend updates to such requirements and language to the FAR Council and other appropriate agencies. The recommendations shall include descriptions of contractors to be covered by the proposed contract language.

(c) The recommended contract language and requirements described in subsection (b) of this section shall be designed to ensure that:

(i) service providers collect and preserve data, information, and reporting relevant to cybersecurity event

prevention, detection, response, and investigation on all information systems over which they have control, including systems operated on behalf of agencies, consistent with agencies' requirements;

(ii) service providers share such data, information, and reporting, as they relate to cyber incidents or potential incidents relevant to any agency with which they have contracted, directly with such agency and any other agency that the Director of OMB, in consultation with the Secretary of Defense, the Attorney General, the Secretary of Homeland Security, and the Director of National Intelligence, deems appropriate, consistent with applicable privacy laws, regulations, and policies;

(iii) service providers collaborate with Federal cybersecurity or investigative agencies in their investigations of and responses to incidents or potential incidents on Federal Information Systems, including by implementing technical capabilities, such as monitoring networks for threats in collaboration with agencies they support, as needed; and

(iv) service providers share cyber threat and incident information with agencies, doing so, where possible, in industry-recognized formats for incident response and remediation.

(d) Within 90 days of receipt of the recommendations described in subsection (b) of this section, the FAR Council shall review the proposed contract language and conditions and, as appropriate, shall publish for public comment proposed updates to the FAR.

(e) Within 120 days of the date of this order, the Secretary of Homeland Security and the Director of OMB shall take appropriate steps to ensure to the greatest extent possible that service providers share data with agencies, CISA, and the FBI as may be necessary for the Federal Government to respond to cyber threats, incidents, and risks.

(f) It is the policy of the Federal Government that:

(i) information and communications technology (ICT) service providers entering into contracts with agencies must promptly report to such agencies when they discover a cyber incident involving a software product or service provided to such agencies or involving a support system for a software product or service provided to such agencies;

(ii) ICT service providers must also directly report to CISA whenever they report under subsection (f)(i) of this section to Federal Civilian Executive Branch (FCEB) Agencies, and CISA must centrally collect and manage such information; and

(iii) reports pertaining to National Security Systems, as defined in section 10(h) of this order, must be received and managed by the appropriate agency as to be determined under subsection (g)(i)(E) of this section.

(g) To implement the policy set forth in subsection (f) of this section:

(i) Within 45 days of the date of this order, the Secretary of Homeland Security, in consultation with the Secretary of Defense acting through the Director of the National Security Agency (NSA), the Attorney General, and the Director of OMB, shall recommend to the FAR Council contract language that identifies:

(A) the nature of cyber incidents that require reporting;

(B) the types of information regarding cyber incidents that require reporting to facilitate effective cyber incident response and remediation;

(C) appropriate and effective protections for privacy and civil liberties;

(D) the time periods within which contractors must report cyber incidents based on a graduated scale of severity, with reporting on the most severe cyber incidents not to exceed 3 days after initial detection;

(E) National Security Systems reporting requirements; and

(F) the type of contractors and associated service providers to be covered by the proposed contract language.

(ii) Within 90 days of receipt of the recommendations described in subsection (g)(i) of this section, the FAR Council shall review the recommendations and publish for public comment proposed updates to the FAR.

(iii) Within 90 days of the date of this order, the Secretary of Defense acting through the Director of the NSA, the Attorney General, the Secretary of Homeland Security, and the Director of National Intelligence shall jointly develop procedures for ensuring that cyber incident reports are promptly and appropriately shared among agencies.

(h) Current cybersecurity requirements for unclassified system contracts are largely implemented through agency-specific policies and regulations, including cloud-service cybersecurity requirements. Standardizing common cybersecurity contractual requirements across agencies will streamline and improve compliance for vendors and the Federal Government.

(i) Within 60 days of the date of this order, the Secretary of Homeland Security acting through the Director of CISA, in consultation with the Secretary of Defense acting through the Director of the NSA, the Director of OMB, and the Administrator of General Services, shall review agency-specific cybersecurity requirements that currently exist as a matter of law, policy, or contract and recommend to the FAR Council standardized contract language for appropriate cybersecurity requirements. Such recommendations shall include consideration of the scope of contractors and associated service providers to be covered by the proposed contract language.

(j) Within 60 days of receiving the recommended contract language developed pursuant to subsection (i) of this section, the FAR Council shall review the recommended contract language and publish for public comment proposed updates to the FAR.

(k) Following any updates to the FAR made by the FAR Council after the public comment period described in subsection (j) of this section, agencies shall update their agency-specific cybersecurity requirements to remove any requirements that are duplicative of such FAR updates.

(l) The Director of OMB shall incorporate into the annual budget process a cost analysis of all recommendations developed under this section.

SEC. 3. *Modernizing Federal Government Cybersecurity.* (a) To keep pace with today's dynamic and increasingly sophisticated cyber threat environment, the Federal Government must take decisive steps to modernize its approach to cybersecurity, including by increasing the Federal Government's visibility into threats, while protecting privacy and civil liberties. The Federal Government must adopt security best practices; advance toward Zero Trust Architecture; accelerate movement to secure cloud services, including Software as a Service (SaaS), Infrastructure as a Service (IaaS), and Platform as a Service (PaaS); centralize and streamline access to cybersecurity data to drive analytics for identifying and managing cybersecurity risks; and invest in both technology and personnel to match these modernization goals.

(b) Within 60 days of the date of this order, the head of each agency shall:

(i) update existing agency plans to prioritize resources for the adoption and use of cloud technology as outlined in relevant OMB guidance;

(ii) develop a plan to implement Zero Trust Architecture, which shall incorporate, as appropriate, the migration steps that the National Institute of Standards and Technology (NIST) within the Department of Commerce has outlined in standards and guidance, describe any such steps that have already been completed, identify activities that will have the most immediate security impact, and include a schedule to implement them; and

(iii) provide a report to the Director of OMB and the Assistant to the President and National Security Advisor (APNSA) discussing the plans required pursuant to subsection (b)(i) and (ii) of this section.

(c) As agencies continue to use cloud technology, they shall do so in a coordinated, deliberate way that allows the Federal Government to prevent, detect, as-

sess, and remediate cyber incidents. To facilitate this approach, the migration to cloud technology shall adopt Zero Trust Architecture, as practicable. The CISA shall modernize its current cybersecurity programs, services, and capabilities to be fully functional with cloud-computing environments with Zero Trust Architecture. The Secretary of Homeland Security acting through the Director of CISA, in consultation with the Administrator of General Services acting through the Federal Risk and Authorization Management Program (FedRAMP) within the General Services Administration, shall develop security principles governing Cloud Service Providers (CSPs) for incorporation into agency modernization efforts. To facilitate this work:

(i) Within 90 days of the date of this order, the Director of OMB, in consultation with the Secretary of Homeland Security acting through the Director of CISA, and the Administrator of General Services acting through FedRAMP, shall develop a Federal cloud-security strategy and provide guidance to agencies accordingly. Such guidance shall seek to ensure that risks to the FCEB from using cloud-based services are broadly understood and effectively addressed, and that FCEB Agencies move closer to Zero Trust Architecture.

(ii) Within 90 days of the date of this order, the Secretary of Homeland Security acting through the Director of CISA, in consultation with the Director of OMB and the Administrator of General Services acting through FedRAMP, shall develop and issue, for the FCEB, cloud-security technical reference architecture documentation that illustrates recommended approaches to cloud migration and data protection for agency data collection and reporting.

(iii) Within 60 days of the date of this order, the Secretary of Homeland Security acting through the Director of CISA shall develop and issue, for FCEB Agencies, a cloud-service governance framework. That framework shall identify a range of services and protections available to agencies based on incident severity. That framework shall also identify data and processing activities associated with those services and protections.

(iv) Within 90 days of the date of this order, the heads of FCEB Agencies, in consultation with the Secretary of Homeland Security acting through the Director of CISA, shall evaluate the types and sensitivity of their respective agency's unclassified data, and shall provide to the Secretary of Homeland Security through the Director of CISA and to the Director of OMB a report based on such evaluation. The evaluation shall prioritize identification of the unclassified data considered by the agency to be the most sensitive and under the greatest threat, and appropriate processing and storage solutions for those data.

(d) Within 180 days of the date of this order, agencies shall adopt multi-factor authentication and encryption for data at rest and in transit, to the maximum extent consistent with Federal records laws and other applicable laws. To that end:

(i) Heads of FCEB Agencies shall provide reports to the Secretary of Homeland Security through the Director of CISA, the Director of OMB, and the APNSA on their respective agency's progress in adopting multi-factor authentication and encryption of data at rest and in transit. Such agencies shall provide such reports every 60 days after the date of this order until the agency has fully adopted, agency-wide, multi-factor authentication and data encryption.

(ii) Based on identified gaps in agency implementation, CISA shall take all appropriate steps to maximize adoption by FCEB Agencies of technologies and processes to implement multifactor authentication and encryption for data at rest and in transit.

(iii) Heads of FCEB Agencies that are unable to fully adopt multi-factor authentication and data encryption within 180 days of the date of this order shall, at the end of the 180-day period, provide a written rationale to the Secretary of Homeland Security through the Director of CISA, the Director of OMB, and the APNSA.

(e) Within 90 days of the date of this order, the Secretary of Homeland Security acting through the Director of CISA, in consultation with the Attorney General, the Director of the FBI, and the Administrator of General Services acting through the Director of FedRAMP, shall establish a framework to collaborate on cybersecurity and incident response activities related to FCEB cloud technology, in order to ensure effective information sharing among agencies and between agencies and CSPs.

(f) Within 60 days of the date of this order, the Administrator of General Services, in consultation with the Director of OMB and the heads of other agencies as the Administrator of General Services deems appropriate, shall begin modernizing FedRAMP by:

(i) establishing a training program to ensure agencies are effectively trained and equipped to manage FedRAMP requests, and providing access to training materials, including videos-on-demand;

(ii) improving communication with CSPs through automation and standardization of messages at each stage of authorization. These communications may include status updates, requirements to complete a vendor's current stage, next steps, and points of contact for questions;

(iii) incorporating automation throughout the lifecycle of FedRAMP, including assessment, authorization, continuous monitoring, and compliance;

(iv) digitizing and streamlining documentation that vendors are required to complete, including through online accessibility and pre-populated forms; and

(v) identifying relevant compliance frameworks, mapping those frameworks onto requirements in the FedRAMP authorization process, and allowing those frameworks to be used as a substitute for the relevant portion of the authorization process, as appropriate.

SEC. 4. *Enhancing Software Supply Chain Security*. (a) The security of software used by the Federal Government is vital to the Federal Government's ability to perform its critical functions. The development of commercial software often lacks transparency, sufficient focus on the ability of the software to resist attack, and adequate controls to prevent tampering by malicious actors. There is a pressing need to implement more rigorous and predictable mechanisms for ensuring that products function securely, and as intended. The security and integrity of ''critical software''—software that performs functions critical to trust (such as affording or requiring elevated system privileges or direct access to networking and computing resources)—is a particular concern. Accordingly, the Federal Government must take action to rapidly improve the security and integrity of the software supply chain, with a priority on addressing critical software.

(b) Within 30 days of the date of this order, the Secretary of Commerce acting through the Director of NIST shall solicit input from the Federal Government, private sector, academia, and other appropriate actors to identify existing or develop new standards, tools, and best practices for complying with the standards, procedures, or criteria in subsection (e) of this section. The guidelines shall include criteria that can be used to evaluate software security, include criteria to evaluate the security practices of the developers and suppliers themselves, and identify innovative tools or methods to demonstrate conformance with secure practices.

(c) Within 180 days of the date of this order, the Director of NIST shall publish preliminary guidelines, based on the consultations described in subsection (b) of this section and drawing on existing documents as practicable, for enhancing software supply chain security and meeting the requirements of this section.

(d) Within 360 days of the date of this order, the Director of NIST shall publish additional guidelines that include procedures for periodic review and updating of the guidelines described in subsection (c) of this section.

(e) Within 90 days of publication of the preliminary guidelines pursuant to subsection (c) of this section, the Secretary of Commerce acting through the Director of NIST, in consultation with the heads of such agencies as the Director of NIST deems appropriate, shall

issue guidance identifying practices that enhance the security of the software supply chain. Such guidance may incorporate the guidelines published pursuant to subsections (c) and (i) of this section. Such guidance shall include standards, procedures, or criteria regarding:

(i) secure software development environments, including such actions as:

(A) using administratively separate build environments;

(B) auditing trust relationships;

(C) establishing multi-factor, risk-based authentication and conditional access across the enterprise;

(D) documenting and minimizing dependencies on enterprise products that are part of the environments used to develop, build, and edit software;

(E) employing encryption for data; and

(F) monitoring operations and alerts and responding to attempted and actual cyber incidents;

(ii) generating and, when requested by a purchaser, providing artifacts that demonstrate conformance to the processes set forth in subsection (e)(i) of this section;

(iii) employing automated tools, or comparable processes, to maintain trusted source code supply chains, thereby ensuring the integrity of the code;

(iv) employing automated tools, or comparable processes, that check for known and potential vulnerabilities and remediate them, which shall operate regularly, or at a minimum prior to product, version, or update release;

(v) providing, when requested by a purchaser, artifacts of the execution of the tools and processes described in subsection (e)(iii) and (iv) of this section, and making publicly available summary information on completion of these actions, to include a summary description of the risks assessed and mitigated;

(vi) maintaining accurate and up-to-date data, provenance (i.e., origin) of software code or components, and controls on internal and third-party software components, tools, and services present in software development processes, and performing audits and enforcement of these controls on a recurring basis;

(vii) providing a purchaser a Software Bill of Materials (SBOM) for each product directly or by publishing it on a public website;

(viii) participating in a vulnerability disclosure program that includes a reporting and disclosure process;

(ix) attesting to conformity with secure software development practices; and

(x) ensuring and attesting, to the extent practicable, to the integrity and provenance of open source software used within any portion of a product.

(f) Within 60 days of the date of this order, the Secretary of Commerce, in coordination with the Assistant Secretary for Communications and Information and the Administrator of the National Telecommunications and Information Administration, shall publish minimum elements for an SBOM.

(g) Within 45 days of the date of this order, the Secretary of Commerce, acting through the Director of NIST, in consultation with the Secretary of Defense acting through the Director of the NSA, the Secretary of Homeland Security acting through the Director of CISA, the Director of OMB, and the Director of National Intelligence, shall publish a definition of the term ''critical software'' for inclusion in the guidance issued pursuant to subsection (e) of this section. That definition shall reflect the level of privilege or access required to function, integration and dependencies with other software, direct access to networking and computing resources, performance of a function critical to trust, and potential for harm if compromised.

(h) Within 30 days of the publication of the definition required by subsection (g) of this section, the Secretary of Homeland Security acting through the Director of CISA, in consultation with the Secretary of Commerce acting through the Director of NIST, shall identify and make available to agencies a list of categories of software and software products in use or in the acquisition process meeting the definition of critical software issued pursuant to subsection (g) of this section.

(i) Within 60 days of the date of this order, the Secretary of Commerce acting through the Director of NIST, in consultation with the Secretary of Homeland Security acting through the Director of CISA and with the Director of OMB, shall publish guidance outlining security measures for critical software as defined in subsection (g) of this section, including applying practices of least privilege, network segmentation, and proper configuration.

(j) Within 30 days of the issuance of the guidance described in subsection (i) of this section, the Director of OMB acting through the Administrator of the Office of Electronic Government within OMB shall take appropriate steps to require that agencies comply with such guidance.

(k) Within 30 days of issuance of the guidance described in subsection (e) of this section, the Director of OMB acting through the Administrator of the Office of Electronic Government within OMB shall take appropriate steps to require that agencies comply with such guidelines with respect to software procured after the date of this order.

(l) Agencies may request an extension for complying with any requirements issued pursuant to subsection (k) of this section. Any such request shall be considered by the Director of OMB on a case-by-case basis, and only if accompanied by a plan for meeting the underlying requirements. The Director of OMB shall on a quarterly basis provide a report to the APNSA identifying and explaining all extensions granted.

(m) Agencies may request a waiver as to any requirements issued pursuant to subsection (k) of this section. Waivers shall be considered by the Director of OMB, in consultation with the APNSA, on a case-by-case basis, and shall be granted only in exceptional circumstances and for limited duration, and only if there is an accompanying plan for mitigating any potential risks.

(n) Within 1 year of the date of this order, the Secretary of Homeland Security, in consultation with the Secretary of Defense, the Attorney General, the Director of OMB, and the Administrator of the Office of Electronic Government within OMB, shall recommend to the FAR Council contract language requiring suppliers of software available for purchase by agencies to comply with, and attest to complying with, any requirements issued pursuant to subsections (g) through (k) of this section.

(o) After receiving the recommendations described in subsection (n) of this section, the FAR Council shall review the recommendations and, as appropriate and consistent with applicable law, amend the FAR.

(p) Following the issuance of any final rule amending the FAR as described in subsection (o) of this section, agencies shall, as appropriate and consistent with applicable law, remove software products that do not meet the requirements of the amended FAR from all indefinite delivery indefinite quantity contracts; Federal Supply Schedules; Federal Government-wide Acquisition Contracts; Blanket Purchase Agreements; and Multiple Award Contracts.

(q) The Director of OMB, acting through the Administrator of the Office of Electronic Government within OMB, shall require agencies employing software developed and procured prior to the date of this order (legacy software) either to comply with any requirements issued pursuant to subsection (k) of this section or to provide a plan outlining actions to remediate or meet those requirements, and shall further require agencies seeking renewals of software contracts, including legacy software, to comply with any requirements issued pursuant to subsection (k) of this section, unless an extension or waiver is granted in accordance with subsection (l) or (m) of this section.

(r) Within 60 days of the date of this order, the Secretary of Commerce acting through the Director of NIST, in consultation with the Secretary of Defense acting through the Director of the NSA, shall publish guidelines recommending minimum standards for ven-

dors' testing of their software source code, including identifying recommended types of manual or automated testing (such as code review tools, static and dynamic analysis, software composition tools, and penetration testing).

(s) The Secretary of Commerce acting through the Director of NIST, in coordination with representatives of other agencies as the Director of NIST deems appropriate, shall initiate pilot programs informed by existing consumer product labeling programs to educate the public on the security capabilities of internet-of-Things (IoT) devices and software development practices, and shall consider ways to incentivize manufacturers and developers to participate in these programs.

(t) Within 270 days of the date of this order, the Secretary of Commerce acting through the Director of NIST, in coordination with the Chair of the Federal Trade Commission (FTC) and representatives of other agencies as the Director of NIST deems appropriate, shall identify IoT cybersecurity criteria for a consumer labeling program, and shall consider whether such a consumer labeling program may be operated in conjunction with or modeled after any similar existing government programs consistent with applicable law. The criteria shall reflect increasingly comprehensive levels of testing and assessment that a product may have undergone, and shall use or be compatible with existing labeling schemes that manufacturers use to inform consumers about the security of their products. The Director of NIST shall examine all relevant information, labeling, and incentive programs and employ best practices. This review shall focus on ease of use for consumers and a determination of what measures can be taken to maximize manufacturer participation.

(u) Within 270 days of the date of this order, the Secretary of Commerce acting through the Director of NIST, in coordination with the Chair of the FTC and representatives from other agencies as the Director of NIST deems appropriate, shall identify secure software development practices or criteria for a consumer software labeling program, and shall consider whether such a consumer software labeling program may be operated in conjunction with or modeled after any similar existing government programs, consistent with applicable law. The criteria shall reflect a baseline level of secure practices, and if practicable, shall reflect increasingly comprehensive levels of testing and assessment that a product may have undergone. The Director of NIST shall examine all relevant information, labeling, and incentive programs, employ best practices, and identify, modify, or develop a recommended label or, if practicable, a tiered software security rating system. This review shall focus on ease of use for consumers and a determination of what measures can be taken to maximize participation.

(v) These pilot programs shall be conducted in a manner consistent with OMB Circular A–119 and NIST Special Publication 2000–02 (Conformity Assessment Considerations for Federal Agencies).

(w) Within 1 year of the date of this order, the Director of NIST shall conduct a review of the pilot programs, consult with the private sector and relevant agencies to assess the effectiveness of the programs, determine what improvements can be made going forward, and submit a summary report to the APNSA.

(x) Within 1 year of the date of this order, the Secretary of Commerce, in consultation with the heads of other agencies as the Secretary of Commerce deems appropriate, shall provide to the President, through the APNSA, a report that reviews the progress made under this section and outlines additional steps needed to secure the software supply chain.

SEC. 5. *Establishing a Cyber Safety Review Board.* (a) The Secretary of Homeland Security, in consultation with the Attorney General, shall establish the Cyber Safety Review Board (Board), pursuant to section 871 of the Homeland Security Act of 2002 (6 U.S.C. 451).

(b) The Board shall review and assess, with respect to significant cyber incidents (as defined under Presidential Policy Directive 41 of July 26, 2016 (United States Cyber Incident Coordination) (PPD–41)) affecting FCEB Information Systems or non-Federal systems, threat activity, vulnerabilities, mitigation activities, and agency responses.

(c) The Secretary of Homeland Security shall convene the Board following a significant cyber incident triggering the establishment of a Cyber Unified Coordination Group (UCG) as provided by section V(B)(2) of PPD–41; at any time as directed by the President acting through the APNSA; or at any time the Secretary of Homeland Security deems necessary.

(d) The Board's initial review shall relate to the cyber activities that prompted the establishment of a UCG in December 2020, and the Board shall, within 90 days of the Board's establishment, provide recommendations to the Secretary of Homeland Security for improving cybersecurity and incident response practices, as outlined in subsection (i) of this section.

(e) The Board's membership shall include Federal officials and representatives from private-sector entities. The Board shall comprise representatives of the Department of Defense, the Department of Justice, CISA, the NSA, and the FBI, as well as representatives from appropriate private-sector cybersecurity or software suppliers as determined by the Secretary of Homeland Security. A representative from OMB shall participate in Board activities when an incident under review involves FCEB Information Systems, as determined by the Secretary of Homeland Security. The Secretary of Homeland Security may invite the participation of others on a case-by-case basis depending on the nature of the incident under review.

(f) The Secretary of Homeland Security shall biennially designate a Chair and Deputy Chair of the Board from among the members of the Board, to include one Federal and one private-sector member.

(g) The Board shall protect sensitive law enforcement, operational, business, and other confidential information that has been shared with it, consistent with applicable law.

(h) The Secretary of Homeland Security shall provide to the President through the APNSA any advice, information, or recommendations of the Board for improving cybersecurity and incident response practices and policy upon completion of its review of an applicable incident.

(i) Within 30 days of completion of the initial review described in subsection (d) of this section, the Secretary of Homeland Security shall provide to the President through the APNSA the recommendations of the Board based on the initial review. These recommendations shall describe:

(i) identified gaps in, and options for, the Board's composition or authorities;

(ii) the Board's proposed mission, scope, and responsibilities;

(iii) membership eligibility criteria for private-sector representatives;

(iv) Board governance structure including interaction with the executive branch and the Executive Office of the President;

(v) thresholds and criteria for the types of cyber incidents to be evaluated;

(vi) sources of information that should be made available to the Board, consistent with applicable law and policy;

(vii) an approach for protecting the information provided to the Board and securing the cooperation of affected United States individuals and entities for the purpose of the Board's review of incidents; and

(viii) administrative and budgetary considerations required for operation of the Board.

(j) The Secretary of Homeland Security, in consultation with the Attorney General and the APNSA, shall review the recommendations provided to the President through the APNSA pursuant to subsection (i) of this section and take steps to implement them as appropriate.

(k) Unless otherwise directed by the President, the Secretary of Homeland Security shall extend the life of

the Board every 2 years as the Secretary of Homeland Security deems appropriate, pursuant to section 871 of the Homeland Security Act of 2002.

SEC. 6. *Standardizing the Federal Government's Playbook for Responding to Cybersecurity Vulnerabilities and Incidents.* (a) The cybersecurity vulnerability and incident response procedures currently used to identify, remediate, and recover from vulnerabilities and incidents affecting their systems vary across agencies, hindering the ability of lead agencies to analyze vulnerabilities and incidents more comprehensively across agencies. Standardized response processes ensure a more coordinated and centralized cataloging of incidents and tracking of agencies' progress toward successful responses.

(b) Within 120 days of the date of this order, the Secretary of Homeland Security acting through the Director of CISA, in consultation with the Director of OMB, the Federal Chief Information Officers Council, and the Federal Chief Information Security Council, and in coordination with the Secretary of Defense acting through the Director of the NSA, the Attorney General, and the Director of National Intelligence, shall develop a standard set of operational procedures (playbook) to be used in planning and conducting a cybersecurity vulnerability and incident response activity respecting FCEB Information Systems. The playbook shall:

(i) incorporate all appropriate NIST standards;

(ii) be used by FCEB Agencies; and

(iii) articulate progress and completion through all phases of an incident response, while allowing flexibility so it may be used in support of various response activities.

(c) The Director of OMB shall issue guidance on agency use of the playbook.

(d) Agencies with cybersecurity vulnerability or incident response procedures that deviate from the playbook may use such procedures only after consulting with the Director of OMB and the APNSA and demonstrating that these procedures meet or exceed the standards proposed in the playbook.

(e) The Director of CISA, in consultation with the Director of the NSA, shall review and update the playbook annually, and provide information to the Director of OMB for incorporation in guidance updates.

(f) To ensure comprehensiveness of incident response activities and build confidence that unauthorized cyber actors no longer have access to FCEB Information Systems, the playbook shall establish, consistent with applicable law, a requirement that the Director of CISA review and validate FCEB Agencies' incident response and remediation results upon an agency's completion of its incident response. The Director of CISA may recommend use of another agency or a third-party incident response team as appropriate.

(g) To ensure a common understanding of cyber incidents and the cybersecurity status of an agency, the playbook shall define key terms and use such terms consistently with any statutory definitions of those terms, to the extent practicable, thereby providing a shared lexicon among agencies using the playbook.

SEC. 7. *Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Networks.* (a) The Federal Government shall employ all appropriate resources and authorities to maximize the early detection of cybersecurity vulnerabilities and incidents on its networks. This approach shall include increasing the Federal Government's visibility into and detection of cybersecurity vulnerabilities and threats to agency networks in order to bolster the Federal Government's cybersecurity efforts.

(b) FCEB Agencies shall deploy an Endpoint Detection and Response (EDR) initiative to support proactive detection of cybersecurity incidents within Federal Government infrastructure, active cyber hunting, containment and remediation, and incident response.

(c) Within 30 days of the date of this order, the Secretary of Homeland Security acting through the Director of CISA shall provide to the Director of OMB recommendations on options for implementing an EDR initiative, centrally located to support host-level visibility, attribution, and response regarding FCEB Information Systems.

(d) Within 90 days of receiving the recommendations described in subsection (c) of this section, the Director of OMB, in consultation with Secretary of Homeland Security, shall issue requirements for FCEB Agencies to adopt Federal Government-wide EDR approaches. Those requirements shall support a capability of the Secretary of Homeland Secretary, acting through the Director of CISA, to engage in cyber hunt, detection, and response activities.

(e) The Director of OMB shall work with the Secretary of Homeland Security and agency heads to ensure that agencies have adequate resources to comply with the requirements issued pursuant to subsection (d) of this section.

(f) Defending FCEB Information Systems requires that the Secretary of Homeland Security acting through the Director of CISA have access to agency data that are relevant to a threat and vulnerability analysis, as well as for assessment and threat-hunting purposes. Within 75 days of the date of this order, agencies shall establish or update Memoranda of Agreement (MOA) with CISA for the Continuous Diagnostics and Mitigation Program to ensure object level data, as defined in the MOA, are available and accessible to CISA, consistent with applicable law.

(g) Within 45 days of the date of this order, the Director of the NSA as the National Manager for National Security Systems (National Manager) shall recommend to the Secretary of Defense, the Director of National Intelligence, and the Committee on National Security Systems (CNSS) appropriate actions for improving detection of cyber incidents affecting National Security Systems, to the extent permitted by applicable law, including recommendations concerning EDR approaches and whether such measures should be operated by agencies or through a centralized service of common concern provided by the National Manager.

(h) Within 90 days of the date of this order, the Secretary of Defense, the Director of National Intelligence, and the CNSS shall review the recommendations submitted under subsection (g) of this section and, as appropriate, establish policies that effectuate those recommendations, consistent with applicable law.

(i) Within 90 days of the date of this order, the Director of CISA shall provide to the Director of OMB and the APNSA a report describing how authorities granted under section 1705 of Public Law 116–283 [amending 44 U.S.C. 3553], to conduct threat-hunting activities on FCEB networks without prior authorization from agencies, are being implemented. This report shall also recommend procedures to ensure that mission-critical systems are not disrupted, procedures for notifying system owners of vulnerable government systems, and the range of techniques that can be used during testing of FCEB Information Systems. The Director of CISA shall provide quarterly reports to the APNSA and the Director of OMB regarding actions taken under section 1705 of Public Law 116–283.

(j) To ensure alignment between Department of Defense Information Network (DODIN) directives and FCEB Information Systems directives, the Secretary of Defense and the Secretary of Homeland Security, in consultation with the Director of OMB, shall:

(i) within 60 days of the date of this order, establish procedures for the Department of Defense and the Department of Homeland Security to immediately share with each other Department of Defense Incident Response Orders or Department of Homeland Security Emergency Directives and Binding Operational Directives applying to their respective information networks;

(ii) evaluate whether to adopt any guidance contained in an Order or Directive issued by the other Department, consistent with regulations concerning sharing of classified information; and

(iii) within 7 days of receiving notice of an Order or Directive issued pursuant to the procedures established under subsection (j)(i) of this section, notify the APNSA and Administrator of the Office of Electronic Government within OMB of the evaluation described in subsection (j)(ii) of this section, including a determination whether to adopt guidance issued by the other Department, the rationale for that determination, and a timeline for application of the directive, if applicable.

SEC. 8. *Improving the Federal Government's Investigative and Remediation Capabilities.* (a) Information from network and system logs on Federal Information Systems (for both on-premises systems and connections hosted by third parties, such as CSPs) is invaluable for both investigation and remediation purposes. It is essential that agencies and their IT service providers collect and maintain such data and, when necessary to address a cyber incident on FCEB Information Systems, provide them upon request to the Secretary of Homeland Security through the Director of CISA and to the FBI, consistent with applicable law.

(b) Within 14 days of the date of this order, the Secretary of Homeland Security, in consultation with the Attorney General and the Administrator of the Office of Electronic Government within OMB, shall provide to the Director of OMB recommendations on requirements for logging events and retaining other relevant data within an agency's systems and networks. Such recommendations shall include the types of logs to be maintained, the time periods to retain the logs and other relevant data, the time periods for agencies to enable recommended logging and security requirements, and how to protect logs. Logs shall be protected by cryptographic methods to ensure integrity once collected and periodically verified against the hashes throughout their retention. Data shall be retained in a manner consistent with all applicable privacy laws and regulations. Such recommendations shall also be considered by the FAR Council when promulgating rules pursuant to section 2 of this order.

(c) Within 90 days of receiving the recommendations described in subsection (b) of this section, the Director of OMB, in consultation with the Secretary of Commerce and the Secretary of Homeland Security, shall formulate policies for agencies to establish requirements for logging, log retention, and log management, which shall ensure centralized access and visibility for the highest level security operations center of each agency.

(d) The Director of OMB shall work with agency heads to ensure that agencies have adequate resources to comply with the requirements identified in subsection (c) of this section.

(e) To address cyber risks or incidents, including potential cyber risks or incidents, the proposed recommendations issued pursuant to subsection (b) of this section shall include requirements to ensure that, upon request, agencies provide logs to the Secretary of Homeland Security through the Director of CISA and to the FBI, consistent with applicable law. These requirements should be designed to permit agencies to share log information, as needed and appropriate, with other Federal agencies for cyber risks or incidents.

SEC. 9. *National Security Systems.* (a) Within 60 days of the date of this order, the Secretary of Defense acting through the National Manager, in coordination with the Director of National Intelligence and the CNSS, and in consultation with the APNSA, shall adopt National Security Systems requirements that are equivalent to or exceed the cybersecurity requirements set forth in this order that are otherwise not applicable to National Security Systems. Such requirements may provide for exceptions in circumstances necessitated by unique mission needs. Such requirements shall be codified in a National Security Memorandum (NSM). Until such time as that NSM is issued, programs, standards, or requirements established pursuant to this order shall not apply with respect to National Security Systems.

(b) Nothing in this order shall alter the authority of the National Manager with respect to National Security Systems as defined in National Security Directive 42 of July 5, 1990 (National Policy for the Security of National Security Telecommunications and Information Systems) (NSD–42). The FCEB network shall continue to be within the authority of the Secretary of Homeland Security acting through the Director of CISA.

SEC. 10. *Definitions.* For purposes of this order:

(a) the term ''agency'' has the meaning ascribed to it under 44 U.S.C. 3502.

(b) the term ''auditing trust relationship'' means an agreed-upon relationship between two or more system elements that is governed by criteria for secure interaction, behavior, and outcomes relative to the protection of assets.

(c) the term ''cyber incident'' has the meaning ascribed to an ''incident'' under 44 U.S.C. 3552(b)(2).

(d) the term ''Federal Civilian Executive Branch Agencies'' or ''FCEB Agencies'' includes all agencies except for the Department of Defense and agencies in the Intelligence Community.

(e) the term ''Federal Civilian Executive Branch Information Systems'' or ''FCEB Information Systems'' means those information systems operated by Federal Civilian Executive Branch Agencies, but excludes National Security Systems.

(f) the term ''Federal Information Systems'' means an information system used or operated by an agency or by a contractor of an agency or by another organization on behalf of an agency, including FCEB Information Systems and National Security Systems.

(g) the term ''Intelligence Community'' or ''IC'' has the meaning ascribed to it under 50 U.S.C. 3003(4).

(h) the term ''National Security Systems'' means information systems as defined in 44 U.S.C. 3552(b)(6), 3553(e)(2), and 3553(e)(3).

(i) the term ''logs'' means records of the events occurring within an organization's systems and networks. Logs are composed of log entries, and each entry contains information related to a specific event that has occurred within a system or network.

(j) the term ''Software Bill of Materials'' or ''SBOM'' means a formal record containing the details and supply chain relationships of various components used in building software. Software developers and vendors often create products by assembling existing open source and commercial software components. The SBOM enumerates these components in a product. It is analogous to a list of ingredients on food packaging. An SBOM is useful to those who develop or manufacture software, those who select or purchase software, and those who operate software. Developers often use available open source and third-party software components to create a product; an SBOM allows the builder to make sure those components are up to date and to respond quickly to new vulnerabilities. Buyers can use an SBOM to perform vulnerability or license analysis, both of which can be used to evaluate risk in a product. Those who operate software can use SBOMs to quickly and easily determine whether they are at potential risk of a newly discovered vulnerability. A widely used, machine-readable SBOM format allows for greater benefits through automation and tool integration. The SBOMs gain greater value when collectively stored in a repository that can be easily queried by other applications and systems. Understanding the supply chain of software, obtaining an SBOM, and using it to analyze known vulnerabilities are crucial in managing risk.

(k) the term ''Zero Trust Architecture'' means a security model, a set of system design principles, and a coordinated cybersecurity and system management strategy based on an acknowledgement that threats exist both inside and outside traditional network boundaries. The Zero Trust security model eliminates implicit trust in any one element, node, or service and instead requires continuous verification of the operational picture via real-time information from multiple sources to determine access and other system responses. In essence, a Zero Trust Architecture allows users full access but only to the bare minimum they

need to perform their jobs. If a device is compromised, zero trust can ensure that the damage is contained. The Zero Trust Architecture security model assumes that a breach is inevitable or has likely already occurred, so it constantly limits access to only what is needed and looks for anomalous or malicious activity. Zero Trust Architecture embeds comprehensive security monitoring; granular risk-based access controls; and system security automation in a coordinated manner throughout all aspects of the infrastructure in order to focus on protecting data in real-time within a dynamic threat environment. This data-centric security model allows the concept of least-privileged access to be applied for every access decision, where the answers to the questions of who, what, when, where, and how are critical for appropriately allowing or denying access to resources based on the combination of sever.

SEC. 11. *General Provisions*. (a) Upon the appointment of the National Cyber Director (NCD) and the establishment of the related Office within the Executive Office of the President, pursuant to section 1752 of Public Law 116–283 [enacting 6 U.S.C. 1500], portions of this order may be modified to enable the NCD to fully execute its duties and responsibilities.

(b) Nothing in this order shall be construed to impair or otherwise affect:

(i) the authority granted by law to an executive department or agency, or the head thereof; or

(ii) the functions of the Director of the Office of Management and Budget relating to budgetary, administrative, or legislative proposals.

(c) This order shall be implemented in a manner consistent with applicable law and subject to the availability of appropriations.

(d) This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

(e) Nothing in this order confers authority to interfere with or to direct a criminal or national security investigation, arrest, search, seizure, or disruption operation or to alter a legal restriction that requires an agency to protect information learned in the course of a criminal or national security investigation.

J.R. BIDEN, JR.

§ 3552. Definitions

(a) IN GENERAL.—Except as provided under subsection (b), the definitions under section 3502 shall apply to this subchapter.

(b) ADDITIONAL DEFINITIONS.—As used in this subchapter:

(1) The term ''binding operational directive'' means a compulsory direction to an agency that—

(A) is for purposes of safeguarding Federal information and information systems from a known or reasonably suspected information security threat, vulnerability, or risk;

(B) shall be in accordance with policies, principles, standards, and guidelines issued by the Director; and

(C) may be revised or repealed by the Director if the direction issued on behalf of the Director is not in accordance with policies and principles developed by the Director.

(2) The term ''incident'' means an occurrence that—

(A) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or

(B) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.

(3) The term ''information security'' means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide—

(A) integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity;

(B) confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and

(C) availability, which means ensuring timely and reliable access to and use of information.

(4) The term ''information technology'' has the meaning given that term in section 11101 of title 40.

(5) The term ''intelligence community'' has the meaning given that term in section 3(4) of the National Security Act of 1947 (50 U.S.C. 3003(4)).

(6)(A) The term ''national security system'' means any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency—

(i) the function, operation, or use of which—

(I) involves intelligence activities;

(II) involves cryptologic activities related to national security;

(III) involves command and control of military forces;

(IV) involves equipment that is an integral part of a weapon or weapons system; or

(V) subject to subparagraph (B), is critical to the direct fulfillment of military or intelligence missions; or

(ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

(B) Subparagraph (A)(i)(V) does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications).

(7) The term ''Secretary'' means the Secretary of Homeland Security.

(Added Pub. L. 113–283, § 2(a), Dec. 18, 2014, 128 Stat. 3074.)

Editorial Notes

PRIOR PROVISIONS

Provisions similar to this section were contained in sections 3532 and 3542 of this title prior to repeal by Pub. L. 113–283.

§ 3553. Authority and functions of the Director and the Secretary

(a) DIRECTOR.—The Director shall oversee agency information security policies and practices, including—

(1) developing and overseeing the implementation of policies, principles, standards, and guidelines on information security, including through ensuring timely agency adoption of and compliance with standards promulgated under section 11331 of title 40;

(2) requiring agencies, consistent with the standards promulgated under such section 11331 and the requirements of this subchapter, to identify and provide information security protections commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of—

(A) information collected or maintained by or on behalf of an agency; or

(B) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency;

(3) ensuring that the Secretary carries out the authorities and functions under subsection (b);

(4) coordinating the development of standards and guidelines under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3) with agencies and offices operating or exercising control of national security systems (including the National Security Agency) to assure, to the maximum extent feasible, that such standards and guidelines are complementary with standards and guidelines developed for national security systems;

(5) overseeing agency compliance with the requirements of this subchapter and section 1326 of title 41, including through any authorized action under section 11303 of title 40, to enforce accountability for compliance with such requirements; and

(6) coordinating information security policies and procedures with related information resources management policies and procedures.

(b) SECRETARY.—The Secretary, in consultation with the Director, shall administer the implementation of agency information security policies and practices for information systems, except for national security systems and information systems described in paragraph (2) or (3) of subsection (e), including—

(1) assisting the Director in carrying out the authorities and functions under paragraphs (1), (2), (3), (5), and (6) of subsection (a);

(2) developing and overseeing the implementation of binding operational directives to agencies to implement the policies, principles, standards, and guidelines developed by the Director under subsection (a)(1) and the requirements of this subchapter, which may be revised or repealed by the Director if the operational directives issued on behalf of the Director are not in accordance with policies, principles, standards, and guidelines developed by the Director, including—

(A) requirements for reporting security incidents to the Federal information security incident center established under section 3556;

(B) requirements for the contents of the annual reports required to be submitted under section 3554(c)(1);

(C) requirements for the mitigation of exigent risks to information systems; and

(D) other operational requirements as the Director or Secretary, in consultation with the Director, may determine necessary;

(3) monitoring agency implementation of information security policies and practices;

(4) convening meetings with senior agency officials to help ensure effective implementation of information security policies and practices;

(5) coordinating Government-wide efforts on information security policies and practices, including consultation with the Chief Information Officers Council established under section 3603 and the Director of the National Institute of Standards and Technology;

(6) providing operational and technical assistance to agencies in implementing policies, principles, standards, and guidelines on information security, including implementation of standards promulgated under section 11331 of title 40, including by—

(A) operating the Federal information security incident center established under section 3556;

(B) upon request by an agency, deploying, operating, and maintaining technology to assist the agency to continuously diagnose and mitigate against cyber threats and vulnerabilities, with or without reimbursement;

(C) compiling and analyzing data on agency information security; and

(D) developing and conducting targeted operational evaluations, including threat and vulnerability assessments, on the information systems;

(7) hunting for and identifying, with or without advance notice to or authorization from agencies, threats and vulnerabilities within Federal information systems;

(8) upon request by an agency, and at the Secretary's discretion, with or without reimbursement—

(A) providing services, functions, and capabilities, including operation of the agency's information security program, to assist the agency with meeting the requirements set forth in section 3554(b); and

(B) deploying, operating, and maintaining secure technology platforms and tools, including networks and common business applications, for use by the agency to perform agency functions, including collecting, maintaining, storing, processing, disseminating, and analyzing information; and

(9) other actions as the Director or the Secretary, in consultation with the Director, may determine necessary to carry out this subsection.

(c) REPORT.—Not later than March 1 of each year, the Director, in consultation with the Secretary, shall submit to Congress a report on the

effectiveness of information security policies and practices during the preceding year, including—

(1) a summary of the incidents described in the annual reports required to be submitted under section 3554(c)(1), including a summary of the information required under section 3554(c)(1)(A)(iii);

(2) a description of the threshold for reporting major information security incidents;

(3) a summary of the results of evaluations required to be performed under section 3555;

(4) an assessment of agency compliance with standards promulgated under section 11331 of title 40; and

(5) an assessment of agency compliance with data breach notification policies and procedures issued by the Director.

(d) NATIONAL SECURITY SYSTEMS.—Except for the authorities and functions described in subsection (a)(5) and subsection (c), the authorities and functions of the Director and the Secretary under this section shall not apply to national security systems.

(e) DEPARTMENT OF DEFENSE AND INTELLIGENCE COMMUNITY SYSTEMS.—(1) The authorities of the Director described in paragraphs (1) and (2) of subsection (a) shall be delegated to the Secretary of Defense in the case of systems described in paragraph (2) and to the Director of National Intelligence in the case of systems described in paragraph (3).

(2) The systems described in this paragraph are systems that are operated by the Department of Defense, a contractor of the Department of Defense, or another entity on behalf of the Department of Defense that processes any information the unauthorized access, use, disclosure, disruption, modification, or destruction of which would have a debilitating impact on the mission of the Department of Defense.

(3) The systems described in this paragraph are systems that are operated by an element of the intelligence community, a contractor of an element of the intelligence community, or another entity on behalf of an element of the intelligence community that processes any information the unauthorized access, use, disclosure, disruption, modification, or destruction of which would have a debilitating impact on the mission of an element of the intelligence community.

(f) CONSIDERATION.—

(1) IN GENERAL.—In carrying out the responsibilities under subsection (b), the Secretary shall consider any applicable standards or guidelines developed by the National Institute of Standards and Technology and issued by the Secretary of Commerce under section 11331 of title 40.

(2) DIRECTIVES.—The Secretary shall—

(A) consult with the Director of the National Institute of Standards and Technology regarding any binding operational directive that implements standards and guidelines developed by the National Institute of Standards and Technology; and

(B) ensure that binding operational directives issued under subsection (b)(2) do not conflict with the standards and guidelines issued under section 11331 of title 40.

(3) RULE OF CONSTRUCTION.—Nothing in this subchapter shall be construed as authorizing the Secretary to direct the Secretary of Commerce in the development and promulgation of standards and guidelines under section 11331 of title 40.

(g) EXERCISE OF AUTHORITY.—To ensure fiscal and policy consistency, the Secretary shall exercise the authority under this section subject to direction by the President, in coordination with the Director.

(h) DIRECTION TO AGENCIES.—

(1) AUTHORITY.—

(A) IN GENERAL.—Subject to subparagraph (B), in response to a known or reasonably suspected information security threat, vulnerability, or incident that represents a substantial threat to the information security of an agency, the Secretary may issue an emergency directive to the head of an agency to take any lawful action with respect to the operation of the information system, including such systems used or operated by another entity on behalf of an agency, that collects, processes, stores, transmits, disseminates, or otherwise maintains agency information, for the purpose of protecting the information system from, or mitigating, an information security threat.

(B) EXCEPTION.—The authorities of the Secretary under this subsection shall not apply to a system described subsection (d) or to a system described in paragraph (2) or (3) of subsection (e).

(2) PROCEDURES FOR USE OF AUTHORITY.—The Secretary shall—

(A) in coordination with the Director, and in consultation with Federal contractors as appropriate, establish procedures governing the circumstances under which a directive may be issued under this subsection, which shall include—

(i) thresholds and other criteria;

(ii) privacy and civil liberties protections; and

(iii) providing notice to potentially affected third parties;

(B) specify the reasons for the required action and the duration of the directive;

(C) minimize the impact of a directive under this subsection by—

(i) adopting the least intrusive means possible under the circumstances to secure the agency information systems; and

(ii) limiting directives to the shortest period practicable;

(D) notify the Director and the head of any affected agency immediately upon the issuance of a directive under this subsection;

(E) consult with the Director of the National Institute of Standards and Technology regarding any directive under this subsection that implements standards and guidelines developed by the National Institute of Standards and Technology;

(F) ensure that directives issued under this subsection do not conflict with the standards and guidelines issued under section 11331 of title 40;

(G) consider any applicable standards or guidelines developed by the National Institute of Standards and Technology issued by the Secretary of Commerce under section 11331 of title 40; and

(H) not later than February 1 of each year, submit to the appropriate congressional committees a report regarding the specific actions the Secretary has taken pursuant to paragraph (1)(A).

(3) IMMINENT THREATS.—

(A) IN GENERAL.—Notwithstanding section 3554, the Secretary may authorize the use under this subsection of the intrusion detection and prevention capabilities established under section 230(b)(1)[1] of the Homeland Security Act of 2002 for the purpose of ensuring the security of agency information systems, if—

(i) the Secretary determines there is an imminent threat to agency information systems;

(ii) the Secretary determines a directive under subsection (b)(2)(C) or paragraph (1)(A) is not reasonably likely to result in a timely response to the threat;

(iii) the Secretary determines the risk posed by the imminent threat outweighs any adverse consequences reasonably expected to result from the use of the intrusion detection and prevention capabilities under the control of the Secretary;

(iv) the Secretary provides prior notice to the Director, and the head and chief information officer (or equivalent official) of each agency to which specific actions will be taken pursuant to this paragraph, and notifies the appropriate congressional committees and authorizing committees of each such agency within 7 days of taking an action under this paragraph of—

(I) any action taken under this paragraph; and

(II) the reasons for and duration and nature of the action;

(v) the action of the Secretary is consistent with applicable law; and

(vi) the Secretary authorizes the use of the intrusion detection and prevention capabilities in accordance with the advance procedures established under subparagraph (C).

(B) LIMITATION ON DELEGATION.—The authority under this paragraph may not be delegated by the Secretary.

(C) ADVANCE PROCEDURES.—The Secretary shall, in coordination with the Director, and in consultation with the heads of Federal agencies, establish procedures governing the circumstances under which the Secretary may authorize the use of the intrusion detection and prevention capabilities under subparagraph (A). The Secretary shall submit the procedures to Congress.

(4) LIMITATION.—The Secretary may direct or authorize lawful action or the use of the intrusion detection and prevention capabilities under this subsection only to—

(A) protect agency information from unauthorized access, use, disclosure, disruption, modification, or destruction; or

(B) require the remediation of or protect against identified information security risks with respect to—

(i) information collected or maintained by or on behalf of an agency; or

(ii) that portion of an information system used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency.

(i) ANNUAL REPORT TO CONGRESS.—Not later than February 1 of each year, the Director and the Secretary shall submit to the appropriate congressional committees a report regarding the specific actions the Director and the Secretary have taken pursuant to subsection (a)(5), including any actions taken pursuant to section 11303(b)(5) of title 40.

(j) RULE OF CONSTRUCTION.—Nothing in this section shall be construed to require the Secretary to provide notice to any private entity before the Secretary issues a binding operational directive under subsection (b)(2).

(k) APPROPRIATE CONGRESSIONAL COMMITTEES DEFINED.—In this section, the term ''appropriate congressional committees'' means—

(1) the Committee on Appropriations and the Committee on Homeland Security and Governmental Affairs of the Senate; and

(2) the Committee on Appropriations, the Committee on Homeland Security, the Committee on Oversight and Government Reform, and the Committee on Science, Space, and Technology of the House of Representatives.

(*l*) INFORMATION SHARING.—

(1) IN GENERAL.—Notwithstanding any other provision of law, including any provision of law that would otherwise restrict or prevent the head of an agency from disclosing information to the Secretary, the Secretary in carrying out this section and title XXII of the Homeland Security Act of 2002 (6 U.S.C. 651 et seq.) may access, use, retain, and disclose, and the head of an agency may disclose to the Secretary, information, for the purpose of protecting information and information systems from cybersecurity risks.

(2) EXCEPTION.—Paragraph (1) shall not apply to national security systems or to information systems described in paragraph (2) or (3) of subsection (e).

(Added Pub. L. 113–283, §2(a), Dec. 18, 2014, 128 Stat. 3075; amended Pub. L. 114–113, div. N, title II, §§224(e), 229(a), Dec. 18, 2015, 129 Stat. 2967, 2972; Pub. L. 115–390, title II, §204(a)(1), Dec. 21, 2018, 132 Stat. 5192; Pub. L. 116–92, div. E, title LXIV, §6432, Dec. 20, 2019, 133 Stat. 2200; Pub. L. 116–283, div. A, title XVII, §1705, Jan. 1, 2021, 134 Stat. 4082.)

Editorial Notes

REFERENCES IN TEXT

Section 230(b)(1) of the Homeland Security Act of 2002, referred to in subsec. (h)(3)(A), is section 230(b)(1) of title II of Pub. L. 107–296, as added by Pub. L. 114–113, div. N, title II, §223(a)(6), Dec. 18, 2015, 129 Stat. 2964, which was redesignated section 2213(b)(1) of Pub. L.

[1] See References in Text note below.

107–296 by section 2(g)(2)(I) of Pub. L. 115–278, Nov. 16, 2018, 132 Stat. 4178, and is classified to section 663(b)(1) of Title 6, Domestic Security.

The Homeland Security Act of 2002, referred to in subsec. (*l*)(1), is Pub. L. 107–296, Nov. 25, 2002, 116 Stat. 2135. Title XXII of the Act is classified generally to subchapter XVIII (§ 651 et seq.) of chapter 1 of Title 6, Domestic Security. For complete classification of this Act to the Code, see Short Title note set out under section 101 of Title 6 and Tables.

PRIOR PROVISIONS

Provisions similar to this section were contained in sections 3533 and 3543 of this title prior to repeal by Pub. L. 113–283.

AMENDMENTS

2021—Subsec. (b)(7) to (9). Pub. L. 116–283, § 1705(1), added pars. (7) and (8) and redesignated former par. (7) as (9).

Subsec. (*l*). Pub. L. 116–283, § 1705(2), added subsec. (*l*).

2019—Subsecs. (j), (k). Pub. L. 116–92 added subsec. (j) and redesignated former subsec. (j) as (k).

2018—Subsec. (a)(5). Pub. L. 115–390 inserted ''and section 1326 of title 41'' after ''compliance with the requirements of this subchapter''.

2015—Subsec. (b)(6)(B). Pub. L. 114–113, § 224(e), inserted '', operating, and maintaining'' after ''deploying''.

Subsecs. (h) to (j). Pub. L. 114–113, § 229(a), added subsecs. (h) to (j).

Statutory Notes and Related Subsidiaries

CHANGE OF NAME

Committee on Oversight and Government Reform of House of Representatives changed to Committee on Oversight and Reform of House of Representatives by House Resolution No. 6, One Hundred Sixteenth Congress, Jan. 9, 2019. Committee on Oversight and Reform of House of Representatives changed to Committee on Oversight and Accountability of House of Representatives by House Resolution No. 5, One Hundred Eighteenth Congress, Jan. 9, 2023.

EFFECTIVE DATE OF 2018 AMENDMENT

Amendment by Pub. L. 115–390 effective 90 days after Dec. 21, 2018, see section 205 of Pub. L. 115–390, set out as an Effective Date note under section 1321 of this title.

CONSTRUCTION

Pub. L. 115–390, title II, § 204(b), Dec. 21, 2018, 132 Stat. 5193, provided that: ''Nothing in this title [see section 201 of Pub. L. 115–390, set out as a Short Title of 2018 note under section 101 of Title 41, Public Contracts] shall be construed to alter or impede any authority or responsibility under section 3553 of title 44, United States Code.''

NO TIKTOK ON GOVERNMENT DEVICES

Pub. L. 117–328, div. R, Dec. 29, 2022, 136 Stat. 5258, provided that:

''SEC. 101. SHORT TITLE.

''This division may be cited as the 'No TikTok on Government Devices Act'.

''SEC. 102. PROHIBITION ON THE USE OF TIKTOK.

''(a) DEFINITIONS.—In this section—

''(1) the term 'covered application' means the social networking service TikTok or any successor application or service developed or provided by ByteDance Limited or an entity owned by ByteDance Limited;

''(2) the term 'executive agency' has the meaning given that term in section 133 of title 41, United States Code; and

''(3) the term 'information technology' has the meaning given that term in section 11101 of title 40, United States Code.

''(b) PROHIBITION ON THE USE OF TIKTOK.—

''(1) IN GENERAL.—Not later than 60 days after the date of the enactment of this Act [Dec. 29, 2022], the Director of the Office of Management and Budget, in consultation with the Administrator of General Services, the Director of the Cybersecurity and Infrastructure Security Agency, the Director of National Intelligence, and the Secretary of Defense, and consistent with the information security requirements under subchapter II of chapter 35 of title 44, United States Code, shall develop standards and guidelines for executive agencies requiring the removal of any covered application from information technology.

''(2) NATIONAL SECURITY AND RESEARCH EXCEPTIONS.—The standards and guidelines developed under paragraph (1) shall include—

''(A) exceptions for law enforcement activities, national security interests and activities, and security researchers; and

''(B) for any authorized use of a covered application under an exception, requirements for executive agencies to develop and document risk mitigation actions for such use.''

BREACHES

Pub. L. 113–283, § 2(d), Dec. 18, 2014, 128 Stat. 3085, provided that:

''(1) REQUIREMENTS.—The Director of the Office of Management and Budget shall ensure that data breach notification policies and guidelines are updated periodically and require—

''(A) except as provided in paragraph (4), notice by the affected agency to each committee of Congress described in section 3554(c)(1) of title 44, United States Code, as added by subsection (a), the Committee on the Judiciary of the Senate, and the Committee on the Judiciary of the House of Representatives, which shall—

''(i) be provided expeditiously and not later than 30 days after the date on which the agency discovered the unauthorized acquisition or access; and

''(ii) include—

''(I) information about the breach, including a summary of any information that the agency knows on the date on which notification is provided about how the breach occurred;

''(II) an estimate of the number of individuals affected by the breach, based on information that the agency knows on the date on which notification is provided, including an assessment of the risk of harm to affected individuals;

''(III) a description of any circumstances necessitating a delay in providing notice to affected individuals; and

''(IV) an estimate of whether and when the agency will provide notice to affected individuals; and

''(B) notice by the affected agency to affected individuals, pursuant to data breach notification policies and guidelines, which shall be provided as expeditiously as practicable and without unreasonable delay after the agency discovers the unauthorized acquisition or access.

''(2) NATIONAL SECURITY; LAW ENFORCEMENT; REMEDIATION.—The Attorney General, the head of an element of the intelligence community (as such term is defined under section 3(4) of the National Security Act of 1947 (50 U.S.C. 3003(4)), or the Secretary of Homeland Security may delay the notice to affected individuals under paragraph (1)(B) if the notice would disrupt a law enforcement investigation, endanger national security, or hamper security remediation actions.

''(3) REPORTS.—

''(A) DIRECTOR OF OMB.—During the first 2 years beginning after the date of enactment of this Act [Dec. 18, 2014], the Director of the Office of Management and Budget shall, on an annual basis—

''(i) assess agency implementation of data breach notification policies and guidelines in aggregate; and

''(ii) include the assessment described in clause (i) in the report required under section 3553(c) of title 44, United States Code.

''(B) SECRETARY OF HOMELAND SECURITY.—During the first 2 years beginning after the date of enactment of this Act, the Secretary of Homeland Security shall include an assessment of the status of agency implementation of data breach notification policies and guidelines in the requirements under section 3553(b)(2)(B) of title 44, United States Code.

''(4) EXCEPTION.—Any element of the intelligence community (as such term is defined under section 3(4) of the National Security Act of 1947 (50 U.S.C. 3003(4)) that is required to provide notice under paragraph (1)(A) shall only provide such notice to appropriate committees of Congress.

''(5) RULE OF CONSTRUCTION.—Nothing in paragraph (1) shall be construed to alter any authority of a Federal agency or department.''

Similar provisions were contained in Pub. L. 113–282, § 7(b), Dec. 18, 2014, 128 Stat. 3071.

§ 3554. Federal agency responsibilities

(a) IN GENERAL.—The head of each agency shall—

(1) be responsible for—

(A) providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of—

(i) information collected or maintained by or on behalf of the agency; and

(ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency;

(B) complying with the requirements of this subchapter, subchapter III of chapter 13 of title 41, and related policies, procedures, standards, and guidelines, including—

(i) information security standards promulgated under section 11331 of title 40;

(ii) operational directives developed by the Secretary under section 3553(b);

(iii) policies and procedures issued by the Director;

(iv) information security standards and guidelines for national security systems issued in accordance with law and as directed by the President;

(v) emergency directives issued by the Secretary under section 3553(h); and

(vi) responsibilities relating to assessing and avoiding, mitigating, transferring, or accepting supply chain risks under section 1326 of title 41, and complying with exclusion and removal orders issued under section 1323 of such title; and

(C) ensuring that information security management processes are integrated with agency strategic, operational, and budgetary planning processes;

(2) ensure that senior agency officials provide information security for the information and information systems that support the operations and assets under their control, including through—

(A) assessing the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of such information or information systems;

(B) determining the levels of information security appropriate to protect such information and information systems in accordance with standards promulgated under section 11331 of title 40, for information security classifications and related requirements;

(C) implementing policies and procedures to cost-effectively reduce risks to an acceptable level; and

(D) periodically testing and evaluating information security controls and techniques to ensure that they are effectively implemented;

(3) delegate to the agency Chief Information Officer established under section 3506 (or comparable official in an agency not covered by such section) the authority to ensure compliance with the requirements imposed on the agency under this subchapter, including—

(A) designating a senior agency information security officer who shall—

(i) carry out the Chief Information Officer's responsibilities under this section;

(ii) possess professional qualifications, including training and experience, required to administer the functions described under this section;

(iii) have information security duties as that official's primary duty; and

(iv) head an office with the mission and resources to assist in ensuring agency compliance with this section;

(B) developing and maintaining an agency-wide information security program as required by subsection (b);

(C) developing and maintaining information security policies, procedures, and control techniques to address all applicable requirements, including those issued under section 3553 of this title and section 11331 of title 40;

(D) training and overseeing personnel with significant responsibilities for information security with respect to such responsibilities; and

(E) assisting senior agency officials concerning their responsibilities under paragraph (2);

(4) ensure that the agency has trained personnel sufficient to assist the agency in complying with the requirements of this subchapter and related policies, procedures, standards, and guidelines;

(5) ensure that the agency Chief Information Officer, in coordination with other senior agency officials, reports annually to the agency head on the effectiveness of the agency information security program, including progress of remedial actions;

(6) ensure that senior agency officials, including chief information officers of component agencies or equivalent officials, carry out responsibilities under this subchapter as directed by the official delegated authority under paragraph (3); and

(7) ensure that all personnel are held accountable for complying with the agency-wide information security program implemented under subsection (b).

(b) AGENCY PROGRAM.—Each agency shall develop, document, and implement an agency-wide information security program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source, that includes—

(1) periodic assessments of the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency, which may include using automated tools consistent with standards and guidelines promulgated under section 11331 of title 40;

(2) policies and procedures that—

(A) are based on the risk assessments required by paragraph (1);

(B) cost-effectively reduce information security risks to an acceptable level;

(C) ensure that information security is addressed throughout the life cycle of each agency information system; and

(D) ensure compliance with—

(i) the requirements of this subchapter;

(ii) policies and procedures as may be prescribed by the Director, and information security standards promulgated under section 11331 of title 40;

(iii) minimally acceptable system configuration requirements, as determined by the agency; and

(iv) any other applicable requirements, including standards and guidelines for national security systems issued in accordance with law and as directed by the President;

(3) subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate;

(4) security awareness training to inform personnel, including contractors and other users of information systems that support the operations and assets of the agency, of—

(A) information security risks associated with their activities; and

(B) their responsibilities in complying with agency policies and procedures designed to reduce these risks;

(5) periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices, to be performed with a frequency depending on risk, but no less than annually, of which such testing—

(A) shall include testing of management, operational, and technical controls of every information system identified in the inventory required under section 3505(c);[1]

(B) may include testing relied on in an evaluation under section 3555; and

(C) shall include using automated tools, consistent with standards and guidelines promulgated under section 11331 of title 40;

(6) a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices of the agency;

(7) procedures for detecting, reporting, and responding to security incidents, which—

(A) shall be consistent with the standards and guidelines described in section 3556(b);

(B) may include using automated tools; and

(C) shall include—

(i) mitigating risks associated with such incidents before substantial damage is done;

(ii) notifying and consulting with the Federal information security incident center established in section 3556; and

(iii) notifying and consulting with, as appropriate—

(I) law enforcement agencies and relevant Offices of Inspector General and Offices of General Counsel;

(II) an office designated by the President for any incident involving a national security system;

(III) for a major incident, the committees of Congress described in subsection (c)(1)—

(aa) not later than 7 days after the date on which there is a reasonable basis to conclude that the major incident has occurred; and

(bb) after the initial notification under item (aa), within a reasonable period of time after additional information relating to the incident is discovered, including the summary required under subsection (c)(1)(A)(i); and

(IV) any other agency or office, in accordance with law or as directed by the President; and

(8) plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency.

(c) AGENCY REPORTING.—

(1) ANNUAL REPORT.—

(A) IN GENERAL.—Each agency shall submit to the Director, the Secretary, the Committee on Government Reform, the Committee on Homeland Security, and the Committee on Science of the House of Representatives, the Committee on Homeland Security and Governmental Affairs and the Committee on Commerce, Science, and Transportation of the Senate, the appropriate authorization and appropriations committees of Congress, and the Comptroller General a report on the adequacy and effectiveness of information security policies, procedures, and practices, including—

(i) a description of each major information security incident or related sets of incidents, including summaries of—

(I) the threats and threat actors, vulnerabilities, and impacts relating to the incident;

(II) the risk assessments conducted under section 3554(a)(2)(A) of the affected information systems before the date on which the incident occurred;

[1] So in original. Section 3505 contains two subsecs. (c).

(III) the status of compliance of the affected information systems with applicable security requirements at the time of the incident; and

(IV) the detection, response, and remediation actions;

(ii) the total number of information security incidents, including a description of incidents resulting in significant compromise of information security, system impact levels, types of incident, and locations of affected systems;

(iii) a description of each major information security incident that involved a breach of personally identifiable information, as defined by the Director, including—

(I) the number of individuals whose information was affected by the major information security incident; and

(II) a description of the information that was breached or exposed; and

(iv) any other information as the Director or the Secretary, in consultation with the Director, may require.

(B) UNCLASSIFIED REPORT.—

(i) IN GENERAL.—Each report submitted under subparagraph (A) shall be in unclassified form, but may include a classified annex.

(ii) ACCESS TO INFORMATION.—The head of an agency shall ensure that, to the greatest extent practicable, information is included in the unclassified version of the reports submitted by the agency under subparagraph (A).

(2) OTHER PLANS AND REPORTS.—Each agency shall address the adequacy and effectiveness of information security policies, procedures, and practices in management plans and reports.

(d) PERFORMANCE PLAN.—(1) In addition to the requirements of subsection (c), each agency, in consultation with the Director, shall include as part of the performance plan required under section 1115 of title 31 a description of—

(A) the time periods; and

(B) the resources, including budget, staffing, and training,

that are necessary to implement the program required under subsection (b).

(2) The description under paragraph (1) shall be based on the risk assessments required under subsection (b)(1).

(e) PUBLIC NOTICE AND COMMENT.—Each agency shall provide the public with timely notice and opportunities for comment on proposed information security policies and procedures to the extent that such policies and procedures affect communication with the public.

(Added Pub. L. 113–283, §2(a), Dec. 18, 2014, 128 Stat. 3078; amended Pub. L. 114–113, div. N, title II, §229(b), Dec. 18, 2015, 129 Stat. 2974; Pub. L. 115–390, title II, §204(a)(2), Dec. 21, 2018, 132 Stat. 5193.)

Editorial Notes

PRIOR PROVISIONS

Provisions similar to this section were contained in sections 3534 and 3544 of this title prior to repeal by Pub. L. 113–283.

AMENDMENTS

2018—Subsec. (a)(1)(B). Pub. L. 115–390, §204(a)(2)(A), inserted '', subchapter III of chapter 13 of title 41,'' after ''complying with the requirements of this subchapter'' in introductory provisions.

Subsec. (a)(1)(B)(vi). Pub. L. 115–390, §204(a)(2)(B), (C), added cl. (vi).

2015—Subsec. (a)(1)(B)(v). Pub. L. 114–113 added cl. (v).

Statutory Notes and Related Subsidiaries

CHANGE OF NAME

Committee on Government Reform of House of Representatives changed to Committee on Oversight and Government Reform of House of Representatives by House Resolution No. 6, One Hundred Tenth Congress, Jan. 5, 2007. Committee on Oversight and Government Reform of House of Representatives changed to Committee on Oversight and Reform of House of Representatives by House Resolution No. 6, One Hundred Sixteenth Congress, Jan. 9, 2019. Committee on Oversight and Reform of House of Representatives changed to Committee on Oversight and Accountability of House of Representatives by House Resolution No. 5, One Hundred Eighteenth Congress, Jan. 9, 2023.

EFFECTIVE DATE OF 2018 AMENDMENT

Amendment by Pub. L. 115–390 effective 90 days after Dec. 21, 2018, see section 205 of Pub. L. 115–390, set out as an Effective Date note under section 1321 of Title 41, Public Contracts.

MAJOR INCIDENT

Pub. L. 113–283, §2(b), Dec. 18, 2014, 128 Stat. 3085, provided that: ''The Director of the Office of Management and Budget shall—

''(1) develop guidance on what constitutes a major incident for purposes of section 3554(b) of title 44, United States Code, as added by subsection (a); and

''(2) provide to Congress periodic briefings on the status of the developing of the guidance until the date on which the guidance is issued.''

§ 3555. Annual independent evaluation

(a) IN GENERAL.—(1) Each year each agency shall have performed an independent evaluation of the information security program and practices of that agency to determine the effectiveness of such program and practices.

(2) Each evaluation under this section shall include—

(A) testing of the effectiveness of information security policies, procedures, and practices of a representative subset of the agency's information systems;

(B) an assessment of the effectiveness of the information security policies, procedures, and practices of the agency; and

(C) separate presentations, as appropriate, regarding information security relating to national security systems.

(b) INDEPENDENT AUDITOR.—Subject to subsection (c)—

(1) for each agency with an Inspector General appointed under chapter 4 of title 5, the annual evaluation required by this section shall be performed by the Inspector General or

by an independent external auditor, as determined by the Inspector General of the agency; and

(2) for each agency to which paragraph (1) does not apply, the head of the agency shall engage an independent external auditor to perform the evaluation.

(c) NATIONAL SECURITY SYSTEMS.—For each agency operating or exercising control of a national security system, that portion of the evaluation required by this section directly relating to a national security system shall be performed—

(1) only by an entity designated by the agency head; and

(2) in such a manner as to ensure appropriate protection for information associated with any information security vulnerability in such system commensurate with the risk and in accordance with all applicable laws.

(d) EXISTING EVALUATIONS.—The evaluation required by this section may be based in whole or in part on an audit, evaluation, or report relating to programs or practices of the applicable agency.

(e) AGENCY REPORTING.—(1) Each year, not later than such date established by the Director, the head of each agency shall submit to the Director the results of the evaluation required under this section.

(2) To the extent an evaluation required under this section directly relates to a national security system, the evaluation results submitted to the Director shall contain only a summary and assessment of that portion of the evaluation directly relating to a national security system.

(f) PROTECTION OF INFORMATION.—Agencies and evaluators shall take appropriate steps to ensure the protection of information which, if disclosed, may adversely affect information security. Such protections shall be commensurate with the risk and comply with all applicable laws and regulations.

(g) OMB REPORTS TO CONGRESS.—(1) The Director shall summarize the results of the evaluations conducted under this section in the report to Congress required under section 3553(c).

(2) The Director's report to Congress under this subsection shall summarize information regarding information security relating to national security systems in such a manner as to ensure appropriate protection for information associated with any information security vulnerability in such system commensurate with the risk and in accordance with all applicable laws.

(3) Evaluations and any other descriptions of information systems under the authority and control of the Director of National Intelligence or of National Foreign Intelligence Programs systems under the authority and control of the Secretary of Defense shall be made available to Congress only through the appropriate oversight committees of Congress, in accordance with applicable laws.

(h) COMPTROLLER GENERAL.—The Comptroller General shall periodically evaluate and report to Congress on—

(1) the adequacy and effectiveness of agency information security policies and practices; and

(2) implementation of the requirements of this subchapter.

(i) ASSESSMENT TECHNICAL ASSISTANCE.—The Comptroller General may provide technical assistance to an Inspector General or the head of an agency, as applicable, to assist the Inspector General or head of an agency in carrying out the duties under this section, including by testing information security controls and procedures.

(j) GUIDANCE.—The Director, in consultation with the Secretary, the Chief Information Officers Council established under section 3603, the Council of the Inspectors General on Integrity and Efficiency, and other interested parties as appropriate, shall ensure the development of guidance for evaluating the effectiveness of an information security program and practices.

(Added Pub. L. 113–283, § 2(a), Dec. 18, 2014, 128 Stat. 3082; amended Pub. L. 117–286, § 4(b)(89), Dec. 27, 2022, 136 Stat. 4352.)

Editorial Notes

PRIOR PROVISIONS

Provisions similar to this section were contained in sections 3535 and 3545 of this title prior to repeal by Pub. L. 113–283.

AMENDMENTS

2022—Subsec. (b)(1). Pub. L. 117–286 substituted ''chapter 4 of title 5,'' for ''the Inspector General Act of 1978,''.

§ 3556. Federal information security incident center

(a) IN GENERAL.—The Secretary shall ensure the operation of a central Federal information security incident center to—

(1) provide timely technical assistance to operators of agency information systems regarding security incidents, including guidance on detecting and handling information security incidents;

(2) compile and analyze information about incidents that threaten information security;

(3) inform operators of agency information systems about current and potential information security threats, and vulnerabilities;

(4) provide, as appropriate, intelligence and other information about cyber threats, vulnerabilities, and incidents to agencies to assist in risk assessments conducted under section 3554(b); and

(5) consult with the National Institute of Standards and Technology, agencies or offices operating or exercising control of national security systems (including the National Security Agency), and such other agencies or offices in accordance with law and as directed by the President regarding information security incidents and related matters.

(b) NATIONAL SECURITY SYSTEMS.—Each agency operating or exercising control of a national security system shall share information about information security incidents, threats, and vulnerabilities with the Federal information security incident center to the extent consistent with standards and guidelines for national security systems, issued in accordance with law and as directed by the President.

(Added Pub. L. 113–283, §2(a), Dec. 18, 2014, 128 Stat. 3084.)

Editorial Notes

PRIOR PROVISIONS

Provisions similar to this section were contained in section 3546 of this title prior to repeal by Pub. L. 113–283.

§ 3557. National security systems

The head of each agency operating or exercising control of a national security system shall be responsible for ensuring that the agency—

(1) provides information security protections commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information contained in such system;

(2) implements information security policies and practices as required by standards and guidelines for national security systems, issued in accordance with law and as directed by the President; and

(3) complies with the requirements of this subchapter.

(Added Pub. L. 113–283, §2(a), Dec. 18, 2014, 128 Stat. 3084.)

Editorial Notes

PRIOR PROVISIONS

Provisions similar to this section were contained in sections 3536 and 3547 of this title prior to repeal by Pub. L. 113–283.

Statutory Notes and Related Subsidiaries

ENFORCEMENT OF CYBERSECURITY REQUIREMENTS FOR NATIONAL SECURITY SYSTEMS

Pub. L. 117–263, div. F, title LXIII, §6309, Dec. 23, 2022, 136 Stat. 3506, as amended by Pub. L. 118–31, div. G, title III, §7352, Dec. 22, 2023, 137 Stat. 1065, provided that:

''(a) DEFINITIONS.—In this section:

''(1) CYBERSECURITY REQUIREMENTS FOR NATIONAL SECURITY SYSTEMS.—The term 'cybersecurity requirements for national security systems' means the minimum cybersecurity requirements established by the National Manager, consistent with the direction of the President and in consultation with the Director of National Intelligence, that applies to all national security systems operated by, on the behalf of, or administered by the head of an element of the intelligence community.

''(2) NATIONAL MANAGER.—The term 'National Manager' means the National Manager for National Security Systems designated by the President.

''(3) NATIONAL SECURITY SYSTEMS.—The term 'national security systems' includes—

''(A) national security systems (as defined in section 3552(b) of title 44, United States Code); and

''(B) information systems described in paragraph (2) or (3) of section 3553(e) of such title.

''(b) IMPLEMENTATION DEADLINE.—The cybersecurity requirements for national security systems shall include appropriate deadlines by which all elements of the intelligence community shall have fully implemented the requirements.

''(c) REEVALUATION AND UPDATES.—Not less frequently than once every 2 years, the National Manager shall reevaluate and update the cybersecurity requirements for national security systems.

''(d) RESOURCES.—Each head of an element of the intelligence community that owns or operates a national security system shall update plans of the element to prioritize resources in such a manner as to fully implement the cybersecurity requirements for national security systems by the deadline established pursuant to subsection (b) for the next 10 fiscal years.

''(e) IMPLEMENTATION REPORT.—Each head of an element of the intelligence community that owns or operates a national security system shall submit to the congressional intelligence committees not later than 90 days after the date of the enactment of this subsection [Dec. 22, 2023] a plan detailing the cost and schedule requirements necessary to meet all of the cybersecurity requirements for national security systems by the end of fiscal year 2026.

''(f) EXEMPTIONS.—

''(1) IN GENERAL.—The head of an element of the intelligence community may exempt a national security system owned or operated by the element from the cybersecurity requirements for national security systems if done so in accordance with the procedures established under paragraph (2).

''(2) EXEMPTION PROCEDURES.—The National Manager shall, consistent with the direction of the President, establish procedures that govern—

''(A) the circumstances under which the head of an element of the intelligence community may exempt a national security system under paragraph (1); and

''(B) the process for implementing the exemption.

''(3) ANNUAL REPORTS ON EXEMPTIONS.—

''(A) IN GENERAL.—Each year, the National Manager and the Director of National Intelligence shall—

''(i) submit to the congressional intelligence committees an annual report documenting all exemptions made under paragraph (1) during the period covered by the report, along with the justifications for the exemptions; and

''(ii) in the case of an exemption made by the Assistant Secretary of State for Intelligence and Research under such paragraph, submit to the Committee on Foreign Relations of the Senate and the Committee on Foreign Affairs of the House of Representatives a separate report describing the exemption and the justification for it.

''(B) MANNER.—Each report submitted under subparagraph (A) shall be submitted with such classification as the Director considers appropriate and with due regard for the protection of sensitive intelligence sources and methods.''

[For definitions of ''intelligence community'' and ''congressional intelligence committees'' as used in section 6309 of Pub. L. 117–263, set out above, see section 3003 of Title 50, War and National Defense, as made applicable by section 6002 of Pub. L. 117–263, which is set out as a note under section 3003 of Title 50.]

§ 3558. Effect on existing law

Nothing in this subchapter, section 11331 of title 40, or section 20 of the National Standards[1] and Technology Act (15 U.S.C. 278g–3) may be construed as affecting the authority of the President, the Office of Management and Budget or the Director thereof, the National Institute of Standards and Technology, or the head of any agency, with respect to the authorized use or disclosure of information, including with regard to the protection of personal privacy under section 552a of title 5, the disclosure of information under section 552 of title 5, the management and disposition of records under chapters[2] 29, 31, or 33 of title 44, the management of information re-

[1] So in original. Probably should be ''National Institute of Standards''.

[2] So in original. Probably should be ''chapter''.

sources under subchapter I of chapter 35 of this title, or the disclosure of information to the Congress or the Comptroller General of the United States.

(Added Pub. L. 113–283, § 2(a), Dec. 18, 2014, 128 Stat. 3084.)

Editorial Notes

PRIOR PROVISIONS

Provisions similar to this section were contained in sections 3538 and 3549 of this title prior to repeal by Pub. L. 113–283.

§ 3559. Federal websites required to be mobile friendly

(a) IN GENERAL.—If, on or after the date that is 180 days after the date of the enactment of this section, an agency creates a website that is intended for use by the public or conducts a redesign of an existing legacy website that is intended for use by the public, the agency shall ensure to the greatest extent practicable that the website is mobile friendly.

(b) DEFINITIONS.—In this section:

(1) AGENCY.—The term ''agency'' has the meaning given that term in section 551 of title 5.

(2) MOBILE FRIENDLY.—The term ''mobile friendly'' means, with respect to a website, that the website is configured in such a way that the website may be navigated, viewed, and accessed on a smartphone, tablet computer, or similar mobile device.

(Added Pub. L. 115–114, § 2(a), Jan. 10, 2018, 131 Stat. 2278.)

Editorial Notes

REFERENCES IN TEXT

The date of the enactment of this section, referred to in subsec. (a), is the date of enactment of Pub. L. 115–114, which was approved Jan. 10, 2018.

SUBCHAPTER III—CONFIDENTIAL INFORMATION PROTECTION AND STATISTICAL EFFICIENCY

Editorial Notes

PRIOR PROVISIONS

Provisions similar to those in parts A to C of this subchapter were contained in Pub. L. 107–347, title V, Dec. 17, 2002, 116 Stat. 2962, which was set out as a note under section 3501 of this title, prior to repeal by Pub. L. 115–435, title III, § 302(c)(1), title IV, § 403, Jan. 14, 2019, 132 Stat. 5552, 5557, effective 180 days after Jan. 14, 2019.

PART A—GENERAL

§ 3561. Definitions

In this subchapter:

(1) AGENCY.—The term ''agency'' means any entity that falls within the definition of the term ''executive agency'', as defined in section 102 of title 31, or ''agency'', as defined in section 3502.

(2) AGENT.—The term ''agent'' means an individual—

(A)(i) who is an employee of a private organization or a researcher affiliated with an institution of higher learning (including a person granted special sworn status by the Bureau of the Census under section 23(c) of title 13), and with whom a contract or other agreement is executed, on a temporary basis, by an executive agency to perform exclusively statistical activities under the control and supervision of an officer or employee of that agency;

(ii) who is working under the authority of a government entity with which a contract or other agreement is executed by an executive agency to perform exclusively statistical activities under the control of an officer or employee of that agency;

(iii) who is a self-employed researcher, a consultant, a contractor, or an employee of a contractor, and with whom a contract or other agreement is executed by an executive agency to perform a statistical activity under the control of an officer or employee of that agency; or

(iv) who is a contractor or an employee of a contractor, and who is engaged by the agency to design or maintain the systems for handling or storage of data received under this subchapter; and

(B) who agrees in writing to comply with all provisions of law that affect information acquired by that agency.

(3) BUSINESS DATA.—The term ''business data'' means operating and financial data and information about businesses, tax-exempt organizations, and government entities.

(4) DATA ASSET.—The term ''data asset'' has the meaning given that term in section 3502.

(5) DIRECTOR.—The term ''Director'' means the Director of the Office of Management and Budget.

(6) EVIDENCE.—The term ''evidence'' means information produced as a result of statistical activities conducted for a statistical purpose.

(7) IDENTIFIABLE FORM.—The term ''identifiable form'' means any representation of information that permits the identity of the respondent to whom the information applies to be reasonably inferred by either direct or indirect means.

(8) NONSTATISTICAL PURPOSE.—The term ''nonstatistical purpose''—

(A) means the use of data in identifiable form for any purpose that is not a statistical purpose, including any administrative, regulatory, law enforcement, adjudicatory, or other purpose that affects the rights, privileges, or benefits of a particular identifiable respondent; and

(B) includes the disclosure under section 552 of title 5 of data that are acquired for exclusively statistical purposes under a pledge of confidentiality.

(9) RESPONDENT.—The term ''respondent'' means a person who, or organization that, is requested or required to supply information to an agency, is the subject of information requested or required to be supplied to an agency, or provides that information to an agency.

(10) STATISTICAL ACTIVITIES.—The term ''statistical activities''—

(A) means the collection, compilation, processing, or analysis of data for the pur-

pose of describing or making estimates concerning the whole, or relevant groups or components within, the economy, society, or the natural environment; and

(B) includes the development of methods or resources that support those activities, such as measurement methods, models, statistical classifications, or sampling frames.

(11) STATISTICAL AGENCY OR UNIT.—The term ''statistical agency or unit'' means an agency or organizational unit of the executive branch whose activities are predominantly the collection, compilation, processing, or analysis of information for statistical purposes, as designated by the Director under section 3562.

(12) STATISTICAL PURPOSE.—The term ''statistical purpose''—

(A) means the description, estimation, or analysis of the characteristics of groups, without identifying the individuals or organizations that comprise such groups; and

(B) includes the development, implementation, or maintenance of methods, technical or administrative procedures, or information resources that support the purposes described in subparagraph (A).

(Added Pub. L. 115–435, title III, §302(a), Jan. 14, 2019, 132 Stat. 5544.)

Statutory Notes and Related Subsidiaries

EFFECTIVE DATE

Section effective 180 days after Jan. 14, 2019, see section 403 of Pub. L. 115–435, set out as an Effective Date of 2019 Amendment note under section 306 of Title 5, Government Organization and Employees.

TRANSITIONAL AND SAVINGS PROVISIONS

Pub. L. 115–435, title III, §302(d), Jan. 14, 2019, 132 Stat. 5553, provided that:

''(1) CUTOFF DATE.—This title [see Short Title of 2019 Amendment note set out under section 101 of this title] replaces certain provisions of law enacted on December 17, 2002. If a law enacted after that date amends or repeals a provision replaced by this title, that law is deemed to amend or repeal, as the case may be, the corresponding provision enacted by this title. If a law enacted after that date is otherwise inconsistent with this title, it supersedes this title to the extent of the inconsistency.

''(2) ORIGINAL DATE OF ENACTMENT UNCHANGED.—For purposes of determining whether one provision of law supersedes another based on enactment later in time, the date of the enactment of a provision enacted by this title is deemed to be the date of the enactment of the provision it replaced.

''(3) REFERENCES TO PROVISIONS REPLACED.—A reference to a provision of law replaced by this title, including a reference in a regulation, order, or other law, is deemed to refer to the corresponding provision enacted by this title.

''(4) REGULATIONS, ORDERS, AND OTHER ADMINISTRATIVE ACTIONS.—A regulation, order, or other administrative action in effect under a provision of law replaced by this title continues in effect under the corresponding provision enacted by this title.

''(5) ACTIONS TAKEN AND OFFENSES COMMITTED.—An action taken or an offense committed under a provision of law replaced by this title is deemed to have been taken or committed under the corresponding provision enacted by this title.''

DEADLINE FOR GUIDANCE AND IMPLEMENTATION

Pub. L. 115–435, title III, §303(c), Jan. 14, 2019, 132 Stat. 5556, provided that: ''Not later than 1 year after the date of the enactment of this Act [Jan. 14, 2019], the Director of the Office of Management and Budget shall promulgate or issue any regulation or guidance required by subchapter III of [chapter 35 of] title 44, United States Code, as amended by this section, with a requirement for such regulation or guidance to be implemented not later than 1 year after the date on which such regulation or guidance has been promulgated or issued.''

§ 3562. Coordination and oversight of policies

(a) IN GENERAL.—The Director shall coordinate and oversee the confidentiality and disclosure policies established by this subchapter. The Director may promulgate rules or provide other guidance to ensure consistent interpretation of this subchapter by the affected agencies. The Director shall develop a process by which the Director designates agencies or organizational units as statistical agencies and units. The Director shall promulgate guidance to implement such process, which shall include specific criteria for such designation and methods by which the Director will ensure transparency in the process.

(b) AGENCY RULES.—Subject to subsection (c), agencies may promulgate rules to implement this subchapter. Rules governing disclosures of information that are authorized by this subchapter shall be promulgated by the agency that originally collected the information.

(c) REVIEW AND APPROVAL OF RULES.—The Director shall review any rules proposed by an agency pursuant to this subchapter for consistency with the provisions of this chapter and such rules shall be subject to the approval of the Director.

(d) REPORTS.—

(1) The head of each agency shall provide to the Director such reports and other information as the Director requests.

(2) Each Designated Statistical Agency (as defined in section 3576(e)) shall report annually to the Director, the Committee on Oversight and Government Reform of the House of Representatives, and the Committee on Homeland Security and Governmental Affairs of the Senate on the actions it has taken to implement section 3576. The report shall include copies of each written agreement entered into pursuant to section 3576(c)(1) for the applicable year.

(3) The Director shall include a summary of reports submitted to the Director under this subsection and actions taken by the Director to advance the purposes of this subchapter in the annual report to Congress on statistical programs prepared under section 3504(e)(2).

(Added Pub. L. 115–435, title III, §302(a), Jan. 14, 2019, 132 Stat. 5546.)

Statutory Notes and Related Subsidiaries

CHANGE OF NAME

Committee on Oversight and Government Reform of House of Representatives changed to Committee on Oversight and Reform of House of Representatives by House Resolution No. 6, One Hundred Sixteenth Congress, Jan. 9, 2019. Committee on Oversight and Reform of House of Representatives changed to Committee on Oversight and Accountability of House of Representatives by House Resolution No. 5, One Hundred Eighteenth Congress, Jan. 9, 2023.

EFFECTIVE DATE

Section effective 180 days after Jan. 14, 2019, see section 403 of Pub. L. 115–435, set out as an Effective Date of 2019 Amendment note under section 306 of Title 5, Government Organization and Employees.

§ 3563. Statistical agencies

(a) RESPONSIBILITIES.—

(1) IN GENERAL.—Each statistical agency or unit shall—

(A) produce and disseminate relevant and timely statistical information;

(B) conduct credible and accurate statistical activities;

(C) conduct objective statistical activities; and

(D) protect the trust of information providers by ensuring the confidentiality and exclusive statistical use of their responses.

(2) POLICIES, BEST PRACTICES, AND PROCEDURES.—Each statistical agency or unit shall adopt policies, best practices, and appropriate procedures to implement the responsibilities described in paragraph (1).

(b) SUPPORT FROM OTHER AGENCIES.—The head of each agency shall enable, support, and facilitate statistical agencies or units in carrying out the responsibilities described in subsection (a)(1).

(c) REGULATIONS.—The Director shall prescribe regulations to carry out this section.

(d) DEFINITIONS.—In this section:

(1) ACCURATE.—The term ''accurate'', when used with respect to statistical activities, means statistics that consistently match the events and trends being measured.

(2) CONFIDENTIALITY.—The term ''confidentiality'' means a quality or condition accorded to information as an obligation not to disclose that information to an unauthorized party.

(3) OBJECTIVE.—The term ''objective'', when used with respect to statistical activities, means accurate, clear, complete, and unbiased.

(4) RELEVANT.—The term ''relevant'', when used with respect to statistical information, means processes, activities, and other such matters likely to be useful to policymakers and public and private sector data users.

(Added Pub. L. 115–435, title III, § 302(a), Jan. 14, 2019, 132 Stat. 5546.)

Statutory Notes and Related Subsidiaries

EFFECTIVE DATE

Section effective 180 days after Jan. 14, 2019, see section 403 of Pub. L. 115–435, set out as an Effective Date of 2019 Amendment note under section 306 of Title 5, Government Organization and Employees.

§ 3564. Effect on other laws

(a) TITLE 44, UNITED STATES CODE.—This subchapter does not diminish the authority under section 3510 of the Director to direct, and of an agency to make, disclosures that are not inconsistent with any applicable law.

(b) TITLE 13 AND TITLE 44, UNITED STATES CODE.—This subchapter does not diminish the authority of the Bureau of the Census to provide information in accordance with sections 8, 16, 301, and 401 of title 13 and section 2108 of this title.

(c) TITLE 13, UNITED STATES CODE.—This subchapter shall not be construed as authorizing the disclosure for nonstatistical purposes of demographic data or information collected by the Bureau of the Census pursuant to section 9 of title 13.

(d) VARIOUS ENERGY STATUTES.—Data or information acquired by the Energy Information Administration under a pledge of confidentiality and designated by the Energy Information Administration to be used for exclusively statistical purposes shall not be disclosed in identifiable form for nonstatistical purposes under—

(1) section 12, 20, or 59 of the Federal Energy Administration Act of 1974 (15 U.S.C. 771, 779, 790h);

(2) section 11 of the Energy Supply and Environmental Coordination Act of 1974 (15 U.S.C. 796); or

(3) section 205 or 407 of the Department of Energy Organization Act (42 U.S.C. 7135, 7177).

(e) SECTION 201 OF CONGRESSIONAL BUDGET ACT OF 1974.—This subchapter shall not be construed to limit any authorities of the Congressional Budget Office to work (consistent with laws governing the confidentiality of information the disclosure of which would be a violation of law) with databases of Designated Statistical Agencies (as defined in section 3576(e)), either separately or, for data that may be shared pursuant to section 3576(c) or other authority, jointly in order to improve the general utility of these databases for the statistical purpose of analyzing pension and health care financing issues.

(f) PREEMPTION OF STATE LAW.—Nothing in this subchapter shall preempt applicable State law regarding the confidentiality of data collected by the States.

(g) STATUTES REGARDING FALSE STATEMENTS.—Notwithstanding section 3572, information collected by an agency for exclusively statistical purposes under a pledge of confidentiality may be provided by the collecting agency to a law enforcement agency for the prosecution of submissions to the collecting agency of false statistical information under statutes that authorize criminal penalties (such as section 221 of title 13) or civil penalties for the provision of false statistical information, unless such disclosure or use would otherwise be prohibited under Federal law.

(h) CONSTRUCTION.—Nothing in this subchapter shall be construed as restricting or diminishing any confidentiality protections or penalties for unauthorized disclosure that otherwise apply to data or information collected for statistical purposes or nonstatistical purposes, including, but not limited to, section 6103 of the Internal Revenue Code of 1986.

(i) AUTHORITY OF CONGRESS.—Nothing in this subchapter shall be construed to affect the authority of the Congress, including its committees, members, or agents, to obtain data or information for a statistical purpose, including for oversight of an agency's statistical activities.

(Added Pub. L. 115–435, title III, § 302(a), Jan. 14, 2019, 132 Stat. 5547.)

Editorial Notes

REFERENCES IN TEXT

Section 201 of the Congressional Budget Act of 1974, referred to in subsec. (e), is classified to section 601 of Title 2, The Congress.

Section 6103 of the Internal Revenue Code of 1986, referred to in subsec. (h), is classified to section 6103 of Title 26, Internal Revenue Code.

Statutory Notes and Related Subsidiaries

EFFECTIVE DATE

Section effective 180 days after Jan. 14, 2019, see section 403 of Pub. L. 115–435, set out as an Effective Date of 2019 Amendment note under section 306 of Title 5, Government Organization and Employees.

PART B—CONFIDENTIAL INFORMATION PROTECTION

§ 3571. Findings

The Congress finds the following:

(1) Individuals, businesses, and other organizations have varying degrees of legal protection when providing information to the agencies for strictly statistical purposes.

(2) Pledges of confidentiality by agencies provide assurances to the public that information about individuals or organizations or provided by individuals or organizations for exclusively statistical purposes will be held in confidence and will not be used against such individuals or organizations in any agency action.

(3) Protecting the confidentiality interests of individuals or organizations who provide information under a pledge of confidentiality for Federal statistical programs serves both the interests of the public and the needs of society.

(4) Declining trust of the public in the protection of information provided under a pledge of confidentiality to the agencies adversely affects both the accuracy and completeness of statistical analyses.

(5) Ensuring that information provided under a pledge of confidentiality for statistical purposes receives protection is essential in continuing public cooperation in statistical programs.

(Added Pub. L. 115–435, title III, § 302(a), Jan. 14, 2019, 132 Stat. 5548.)

Statutory Notes and Related Subsidiaries

EFFECTIVE DATE

Section effective 180 days after Jan. 14, 2019, see section 403 of Pub. L. 115–435, set out as an Effective Date of 2019 Amendment note under section 306 of Title 5, Government Organization and Employees.

§ 3572. Confidential information protection

(a) PURPOSES.—The purposes of this section are the following:

(1) To ensure that information supplied by individuals or organizations to an agency for statistical purposes under a pledge of confidentiality is used exclusively for statistical purposes.

(2) To ensure that individuals or organizations who supply information under a pledge of confidentiality to agencies for statistical purposes will neither have that information disclosed in identifiable form to anyone not authorized by this subchapter nor have that information used for any purpose other than a statistical purpose.

(3) To safeguard the confidentiality of individually identifiable information acquired under a pledge of confidentiality for statistical purposes by controlling access to, and uses made of, such information.

(b) USE OF STATISTICAL DATA OR INFORMATION.—Data or information acquired by an agency under a pledge of confidentiality and for exclusively statistical purposes shall be used by officers, employees, or agents of the agency exclusively for statistical purposes and protected in accordance with such pledge.

(c) DISCLOSURE OF STATISTICAL DATA OR INFORMATION.—

(1) Data or information acquired by an agency under a pledge of confidentiality for exclusively statistical purposes shall not be disclosed by an agency in identifiable form, for any use other than an exclusively statistical purpose, except with the informed consent of the respondent.

(2) A disclosure pursuant to paragraph (1) is authorized only when the head of the agency approves such disclosure and the disclosure is not prohibited by any other law.

(3) This section does not restrict or diminish any confidentiality protections in law that otherwise apply to data or information acquired by an agency under a pledge of confidentiality for exclusively statistical purposes.

(d) RULE FOR USE OF DATA OR INFORMATION FOR NONSTATISTICAL PURPOSES.—A statistical agency or unit shall clearly distinguish any data or information it collects for nonstatistical purposes (as authorized by law) and provide notice to the public, before the data or information is collected, that the data or information could be used for nonstatistical purposes.

(e) DESIGNATION OF AGENTS.—A statistical agency or unit may designate agents, by contract or by entering into a special agreement containing the provisions required under section 3561(2) for treatment as an agent under that section, who may perform exclusively statistical activities, subject to the limitations and penalties described in this subchapter.

(f) FINES AND PENALTIES.—Whoever, being an officer, employee, or agent of an agency acquiring information for exclusively statistical purposes, having taken and subscribed the oath of office, or having sworn to observe the limitations imposed by this section, comes into possession of such information by reason of his or her being an officer, employee, or agent and, knowing that the disclosure of the specific information is prohibited under the provisions of this subchapter, willfully discloses the information in any manner to a person or agency not entitled to receive it, shall be guilty of a class E felony and imprisoned for not more than 5 years, or fined not more than $250,000, or both.

(Added Pub. L. 115–435, title III, § 302(a), Jan. 14, 2019, 132 Stat. 5548.)

Statutory Notes and Related Subsidiaries

EFFECTIVE DATE

Section effective 180 days after Jan. 14, 2019, see section 403 of Pub. L. 115–435, set out as an Effective Date of 2019 Amendment note under section 306 of Title 5, Government Organization and Employees.

PART C—STATISTICAL EFFICIENCY

§ 3575. Findings

The Congress finds the following:

(1) Federal statistics are an important source of information for public and private decision-makers such as policymakers, consumers, businesses, investors, and workers.

(2) Federal statistical agencies should continuously seek to improve their efficiency. Statutory constraints limit the ability of these agencies to share data and thus to achieve higher efficiency for Federal statistical programs.

(3) The quality of Federal statistics depends on the willingness of businesses to respond to statistical surveys. Reducing reporting burdens will increase response rates, and therefore lead to more accurate characterizations of the economy.

(4) Enhanced sharing of business data among the Bureau of the Census, the Bureau of Economic Analysis, and the Bureau of Labor Statistics for exclusively statistical purposes will improve their ability to track more accurately the large and rapidly changing nature of United States business. In particular, the statistical agencies will be able to better ensure that businesses are consistently classified in appropriate industries, resolve data anomalies, produce statistical samples that are consistently adjusted for the entry and exit of new businesses in a timely manner, and correct faulty reporting errors quickly and efficiently.

(5) Congress enacted the International Investment and Trade in Services Survey Act (Public Law 94–472), which allowed the Bureau of the Census, the Bureau of Economic Analysis, and the Bureau of Labor Statistics to share data on foreign-owned companies. The Act not only expanded detailed industry coverage from 135 industries to over 800 industries with no increase in the data collected from respondents but also demonstrated how data sharing can result in the creation of valuable data products.

(6) With part B of this subchapter, the sharing of business data among the Bureau of the Census, the Bureau of Economic Analysis, and the Bureau of Labor Statistics continues to ensure the highest level of confidentiality for respondents to statistical surveys.

(Added Pub. L. 115–435, title III, § 302(a), Jan. 14, 2019, 132 Stat. 5549.)

Editorial Notes

REFERENCES IN TEXT

The International Investment and Trade in Services Survey Act, referred to in par. (5), is Pub. L. 94–472, Oct. 11, 1976, 90 Stat. 2059, which is classified generally to chapter 46 (§ 3101 et seq.) of Title 22, Foreign Relations and Intercourse. For complete classification of this Act to the Code, see Short Title note set out under section 3101 of Title 22 and Tables.

Statutory Notes and Related Subsidiaries

EFFECTIVE DATE

Section effective 180 days after Jan. 14, 2019, see section 403 of Pub. L. 115–435, set out as an Effective Date of 2019 Amendment note under section 306 of Title 5, Government Organization and Employees.

§ 3576. Designated statistical agencies

(a) PURPOSES.—The purposes of this section are the following:

(1) To authorize the sharing of business data among the Bureau of the Census, the Bureau of Economic Analysis, and the Bureau of Labor Statistics for exclusively statistical purposes.

(2) To reduce the paperwork burdens imposed on businesses that provide requested information to the Federal Government.

(3) To improve the comparability and accuracy of Federal economic statistics by allowing the Bureau of the Census, the Bureau of Economic Analysis, and the Bureau of Labor Statistics to update sample frames, develop consistent classifications of establishments and companies into industries, improve coverage, and reconcile significant differences in data produced by the three agencies.

(4) To increase understanding of the United States economy, especially for key industry and regional statistics, to develop more accurate measures of the impact of technology on productivity growth, and to enhance the reliability of the Nation's most important economic indicators, such as the National Income and Product Accounts.

(b) RESPONSIBILITIES OF DESIGNATED STATISTICAL AGENCIES.—The head of each of the Designated Statistical Agencies shall—

(1) identify opportunities to eliminate duplication and otherwise reduce reporting burden and cost imposed on the public in providing information for statistical purposes;

(2) enter into joint statistical projects to improve the quality and reduce the cost of statistical programs; and

(3) protect the confidentiality of individually identifiable information acquired for statistical purposes by adhering to safeguard principles, including—

(A) emphasizing to their officers, employees, and agents the importance of protecting the confidentiality of information in cases where the identity of individual respondents can reasonably be inferred by either direct or indirect means;

(B) training their officers, employees, and agents in their legal obligations to protect the confidentiality of individually identifiable information and in the procedures that must be followed to provide access to such information;

(C) implementing appropriate measures to assure the physical and electronic security of confidential data;

(D) establishing a system of records that identifies individuals accessing confidential

data and the project for which the data were required; and

(E) being prepared to document their compliance with safeguard principles to other agencies authorized by law to monitor such compliance.

(c) SHARING OF BUSINESS DATA AMONG DESIGNATED STATISTICAL AGENCIES.—

(1) IN GENERAL.—A Designated Statistical Agency may provide business data in an identifiable form to another Designated Statistical Agency under the terms of a written agreement among the agencies sharing the business data that specifies—

(A) the business data to be shared;

(B) the statistical purposes for which the business data are to be used;

(C) the officers, employees, and agents authorized to examine the business data to be shared; and

(D) appropriate security procedures to safeguard the confidentiality of the business data.

(2) RESPONSIBILITIES OF AGENCIES UNDER OTHER LAWS.—The provision of business data by an agency to a Designated Statistical Agency under this section shall in no way alter the responsibility of the agency providing the data under other statutes (including sections 552 and 552b of title 5) with respect to the provision or withholding of such information by the agency providing the data.

(3) RESPONSIBILITIES OF OFFICERS, EMPLOYEES, AND AGENTS.—Examination of business data in identifiable form shall be limited to the officers, employees, and agents authorized to examine the individual reports in accordance with written agreements pursuant to this section. Officers, employees, and agents of a Designated Statistical Agency who receive data pursuant to this section shall be subject to all provisions of law, including penalties, that relate—

(A) to the unlawful provision of the business data that would apply to the officers, employees, and agents of the agency that originally obtained the information; and

(B) to the unlawful disclosure of the business data that would apply to officers, employees, and agents of the agency that originally obtained the information.

(4) NOTICE.—Whenever a written agreement concerns data that respondents were required by law to report and the respondents were not informed that the data could be shared among the Designated Statistical Agencies, for exclusively statistical purposes, the terms of such agreement shall be described in a public notice issued by the agency that intends to provide the data. Such notice shall allow a minimum of 60 days for public comment.

(d) LIMITATIONS ON USE OF BUSINESS DATA PROVIDED BY DESIGNATED STATISTICAL AGENCIES.—

(1) GENERAL USE.—Business data provided by a Designated Statistical Agency pursuant to this section shall be used exclusively for statistical purposes.

(2) PUBLICATION.—Publication of business data acquired by a Designated Statistical Agency shall occur in a manner whereby the data furnished by any particular respondent are not in identifiable form.

(e) DESIGNATED STATISTICAL AGENCY DEFINED.—In this section, the term ''Designated Statistical Agency'' means each of the following:

(1) The Census Bureau of the Department of Commerce.

(2) The Bureau of Economic Analysis of the Department of Commerce.

(3) The Bureau of Labor Statistics of the Department of Labor.

(Added Pub. L. 115–435, title III, § 302(a), Jan. 14, 2019, 132 Stat. 5550.)

Statutory Notes and Related Subsidiaries

EFFECTIVE DATE

Section effective 180 days after Jan. 14, 2019, see section 403 of Pub. L. 115–435, set out as an Effective Date of 2019 Amendment note under section 306 of Title 5, Government Organization and Employees.

PART D—ACCESS TO DATA FOR EVIDENCE

§ 3581. Presumption of accessibility for statistical agencies and units

(a) ACCESSIBILITY OF DATA ASSETS.—The head of an agency shall, to the extent practicable, make any data asset maintained by the agency available, upon request, to any statistical agency or unit for purposes of developing evidence.

(b) LIMITATIONS.—Subsection (a) does not apply to any data asset that is subject to a statute that—

(1) prohibits the sharing or intended use of such asset in a manner as to leave no discretion on the issue; or

(2) if enacted after the date of the enactment of this section, specifically cites to this paragraph.

(c) REGULATIONS.—The Director shall prescribe regulations for agencies to carry out this section. Such regulations shall—

(1) require the timely provision of data assets under subsection (a);

(2) provide a list of statutes that exempt agencies from the requirement under subsection (a) pursuant to subsection (b)(1);

(3) establish clear and consistent standards, to the extent possible, for complying with section 552a of title 5 (commonly known as the ''Privacy Act of 1974'') and any other applicable law requiring the protection and confidentiality of individually identifiable information; and

(4) require a transparent process for statistical agencies and units to request data assets from agencies and for agencies to respond to such requests.

(d) RULE OF CONSTRUCTION.—Nothing in this section may be construed as altering existing intellectual property rights or the terms of any contract or other binding, written agreement.

(Added Pub. L. 115–435, title III, § 303(a), Jan. 14, 2019, 132 Stat. 5554.)

Editorial Notes

REFERENCES IN TEXT

The date of the enactment of this section, referred to in subsec. (b)(2), is the date of enactment of Pub. L. 115–435, which was approved Jan. 14, 2019.

Statutory Notes and Related Subsidiaries

EFFECTIVE DATE

Section effective 180 days after Jan. 14, 2019, see section 403 of Pub. L. 115–435, set out as an Effective Date of 2019 Amendment note under section 306 of Title 5, Government Organization and Employees.

§ 3582. Expanding secure access to CIPSEA data assets

(a) STATISTICAL AGENCY RESPONSIBILITIES.—To the extent practicable, each statistical agency or unit shall expand access to data assets of such agency or unit acquired or accessed under this subchapter to develop evidence while protecting such assets from inappropriate access and use, in accordance with the regulations promulgated under subsection (b).

(b) REGULATIONS FOR ACCESSIBILITY OF NONPUBLIC DATA ASSETS.—The Director shall promulgate regulations, in accordance with applicable law, for statistical agencies and units to carry out the requirement under subsection (a). Such regulations shall include the following:

(1) Standards for each statistical agency or unit to assess each data asset owned or accessed by the statistical agency or unit for purposes of categorizing the sensitivity level of each such asset and identifying the corresponding level of accessibility to each such asset. Such standards shall include—

(A) common sensitivity levels and corresponding levels of accessibility that may be assigned to a data asset, including a requisite minimum and maximum number of sensitivity levels for each statistical agency or unit to use;

(B) criteria for determining the sensitivity level and corresponding level of accessibility of each data asset; and

(C) criteria for determining whether a less sensitive and more accessible version of a data asset can be produced.

(2) Standards for each statistical agency or unit to improve access to a data asset pursuant to paragraph (1) or (3) by removing or obscuring information in such a manner that the identity of the data subject is less likely to be reasonably inferred by either direct or indirect means.

(3) A requirement for each statistical agency or unit to conduct a comprehensive risk assessment of any data asset acquired or accessed under this subchapter prior to any public release of such asset, including standards for such comprehensive risk assessment and criteria for making a determination of whether to release the data.

(4) Requirements for each statistical agency or unit to make any process or assessment established, produced, or conducted pursuant to this section transparent and easy to understand, including the following:

(A) A requirement to make information on the assessment of the sensitivity level of each data asset conducted pursuant to paragraph (1) available on the Federal data catalogue established under section 3511(c)(1).

(B) A requirement to make any comprehensive risk assessment, and associated determinations, conducted under paragraph (3) available on the Federal data catalogue established under section 3511(c)(1).

(C) A requirement to make any standard or policy established by the statistical agency or unit to carry out this section and any assessment conducted under this section easily accessible on the public website of such agency or unit.

(c) RESPONSIBILITIES OF THE DIRECTOR.—The Director shall—

(1) make public all standards and policies established under this section; and

(2) ensure that statistical agencies and units have the ability to make information public on the Federal data catalogue established under section 3511(c)(1), in accordance with requirements established pursuant to subsection (b).

(Added Pub. L. 115–435, title III, § 303(a), Jan. 14, 2019, 132 Stat. 5554.)

Statutory Notes and Related Subsidiaries

EFFECTIVE DATE

Section effective 180 days after Jan. 14, 2019, see section 403 of Pub. L. 115–435, set out as an Effective Date of 2019 Amendment note under section 306 of Title 5, Government Organization and Employees.

§ 3583. Application to access data assets for developing evidence

(a) STANDARD APPLICATION PROCESS.—The Director shall establish a process through which agencies, the Congressional Budget Office, State, local, and Tribal governments, researchers, and other individuals, as appropriate, may apply to access the data assets accessed or acquired under this subchapter by a statistical agency or unit for purposes of developing evidence. The process shall include the following:

(1) Sufficient detail to ensure that each statistical agency or unit establishes an identical process.

(2) A common application form.

(3) Criteria for statistical agencies and units to determine whether to grant an applicant access to a data asset.

(4) Timeframes for prompt determinations by each statistical agency or unit.

(5) An appeals process for adverse decisions and noncompliance with the process established under this subsection.

(6) Standards for transparency, including requirements to make the following information publicly available:

(A) Each application received.

(B) The status of each application.

(C) The determination made for each application.

(D) Any other information, as appropriate, to ensure full transparency of the process established under this subsection.

(b) CONSULTATION.—In establishing the process required under subsection (a), the Director shall

consult with stakeholders, including the public, agencies, State and local governments, and representatives of non-governmental researchers.

(c) IMPLEMENTATION.—The head of each statistical agency or unit shall implement the process established under subsection (a).

(Added Pub. L. 115–435, title III, § 303(a), Jan. 14, 2019, 132 Stat. 5555.)

Statutory Notes and Related Subsidiaries

EFFECTIVE DATE

Section effective 180 days after Jan. 14, 2019, see section 403 of Pub. L. 115–435, set out as an Effective Date of 2019 Amendment note under section 306 of Title 5, Government Organization and Employees.

CHAPTER 36—MANAGEMENT AND PROMOTION OF ELECTRONIC GOVERNMENT SERVICES

AMENDMENT OF ANALYSIS

Pub. L. 117–263, div. E, title LIX, § 5921(d)(2), Dec. 23, 2022, 136 Stat. 3458, provided that, effective on the date that is 5 years after Dec. 23, 2022, this analysis is amended by striking items 3607 to 3616.

Editorial Notes

AMENDMENTS

2022—Pub. L. 117–263, div. E, title LIX, § 5921(d)(2), Dec. 23, 2022, 136 Stat. 3458, struck out items 3607 ''Definitions'', 3608 ''Federal Risk and Authorization Management Program'', 3609 ''Roles and responsibilities of the General Services Administration'', 3610 ''FedRAMP Board'', 3611 ''Independent assessment'', 3612 ''Declaration of foreign interests'', 3613 ''Roles and responsibilities of agencies'', 3614 ''Roles and responsibilities of the Office of Management and Budget'', 3615 ''Reports to Congress; GAO report'', and 3616 ''Federal Secure Cloud Advisory Committee''. See Effective Date of 2022 Amendment note below.

Pub. L. 117–263, div. E, title LIX, § 5921(c), Dec. 23, 2022, 136 Stat. 3458, added items 3607 to 3616.

Statutory Notes and Related Subsidiaries

EFFECTIVE DATE OF 2022 AMENDMENT

Pub. L. 117–263, div. E, title LIX, § 5921(d)(2), Dec. 23, 2022, 136 Stat. 3458, provided that, effective on the date that is 5 years after Dec. 23, 2022, this analysis is amended by striking items 3607 to 3616.

§ 3601. Definitions

In this chapter, the definitions under section 3502 shall apply, and the term—

(1) ''Administrator'' means the Administrator of the Office of Electronic Government established under section 3602;

(2) ''Council'' means the Chief Information Officers Council established under section 3603;

(3) ''electronic Government'' means the use by the Government of web-based Internet applications and other information technologies, combined with processes that implement these technologies, to—

(A) enhance the access to and delivery of Government information and services to the public, other agencies, and other Government entities; or

(B) bring about improvements in Government operations that may include effectiveness, efficiency, service quality, or transformation;

(4) ''enterprise architecture''—

(A) means—

(i) a strategic information asset base, which defines the mission;

(ii) the information necessary to perform the mission;

(iii) the technologies necessary to perform the mission; and

(iv) the transitional processes for implementing new technologies in response to changing mission needs; and

(B) includes—

(i) a baseline architecture;

(ii) a target architecture; and

(iii) a sequencing plan;

(5) ''Fund'' means the E-Government Fund established under section 3604;

(6) ''interoperability'' means the ability of different operating and software systems, applications, and services to communicate and exchange data in an accurate, effective, and consistent manner;

(7) ''integrated service delivery'' means the provision of Internet-based Federal Government information or services integrated according to function or topic rather than separated according to the boundaries of agency jurisdiction; and

(8) ''tribal government'' means—

(A) the governing body of any Indian tribe, band, nation, or other organized group or community located in the continental United States (excluding the State of Alaska) that is recognized as eligible for the special programs and services provided by the United States to Indians because of their status as Indians, and

(B) any Alaska Native regional or village corporation established pursuant to the Alaska Native Claims Settlement Act (43 U.S.C. 1601 et seq.).

(Added Pub. L. 107–347, title I, § 101(a), Dec. 17, 2002, 116 Stat. 2901.)

Editorial Notes

REFERENCES IN TEXT

The Alaska Native Claims Settlement Act, referred to in par. (8)(B), is Pub. L. 92–203, Dec. 18, 1971, 85 Stat. 688, which is classified generally to chapter 33 (§ 1601 et seq.) of Title 43, Public Lands. For complete classification of this Act to the Code, see Short Title note set out under section 1601 of Title 43 and Tables.