2. Laws

2.1 Federal Information Technology Acquisition Reform Act (2014)

The Federal Information Technology Acquisition Reform Act (FITARA), passed in December 2014, strengthened the role of agency CIOs and provided greater accountability for the delivery of IT capabilities across the Federal Government. To assist with agency implementation, OMB released OMB Memorandum M-15-14: Management and Oversight of Federal Information Technology[172] in June 2015.

FITARA outlines specific requirements related to:

1. Agency CIO Authority Enhancements
2. Enhanced Transparency and Improved Risk Management in IT Investments
3. Portfolio Review
4. Data Center Consolidation Initiative[173]
5. Expansion of Training and Use of IT Cadres
6. Maximizing the Benefit of the Federal Strategic Sourcing Initiative
7. Governmentwide Software Purchasing Program

Among other provisions, FITARA codified elements of existing Federal CIO initiatives. In addition, FITARA requires the Federal CIO, in conjunction with federal agencies, to:

- Refocus the Federal Data Center Consolidation Initiative (FDCCI) from consolidation to optimization, to include adoption of cloud services;
- Set forth a process for agency IT portfolio review and oversight;
- Improve transparency and risk management of IT investments;
- Identify and publish cost savings and optimization improvements;
- Provide public updates on cumulative cost savings and optimization improvements; and
- Review agencies' data center inventories and management strategies.

FITARA requires federal agencies to submit annual reports that include:

- Comprehensive data center inventories,
- Multiyear strategies to consolidate and optimize data centers,
- Performance metrics and a timeline for agency action, and
- Yearly calculations of investment and cost savings related to FITARA implementation.[174]

See Reporting Calendar for additional information on FITARA reporting activities.

[172] OMB M-15-14. Management and Oversight of Federal Information Technology. 6/10/2015. https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2015/m-15-14.pdf
[173] OMB M-19-19. Update to Data Center Optimization Initiative (DCOI). 6/25/2019. https://datacenters.cio.gov/assets/files/m_19_19.pdf
[174] Congressional Research Service. The Current State of Federal Information Technology Acquisition Reform and Management. 2/03/2020. https://fas.org/sgp/crs/misc/R44843.pdf

Figure 1 identifies twelve practices,[175] including four overarching ones, considered vital to implementing FITARA published by GAO.

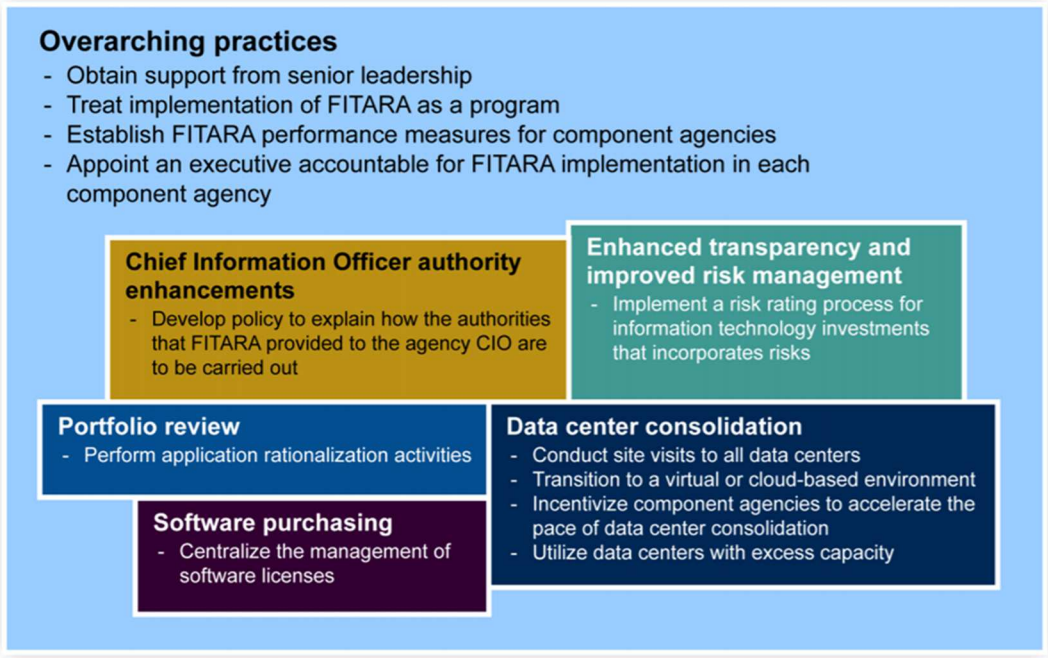

Figure 1: Practices for Effectively Implementing FITARA

2.2 Clinger Cohen Act (1996)

The Information Technology Management Reform Act (ITMRA) and the Federal Acquisition Reform Act (FARA) were signed into law as part of the National Defense Authorization Act for Fiscal Year 1996 and were subsequently designated the Clinger Cohen Act of 1996. This was the first time in law that agency CIO positions were established with designated roles and responsibilities. Clinger Cohen also directs Federal agencies to focus more on the results achieved through IT investments and streamlined the Federal IT procurement process, detailing how agencies approach the selection and management of IT projects.[176]

As part of the law, OMB is required to establish a budget process for analyzing, tracking, and evaluating, the risks and results of IT projects. This guidance has evolved and now encompasses the annual CPIC budget process. In addition, OMB was required to perform review of information resources management activities and ensure that adequate information security policies and procedures are in place across Federal agencies.

[175] GAO-19-131. Effective Practices Have Improved Agencies' FITARA Implementation. April 2019. https://www.gao.gov/assets/700/698751.pdf

[176] DOD. Department of Defense Chief Information Officer Desk Reference. 2006. https://dodcio.defense.gov/Portals/0/Documents/ciodesrefvolone.pdf

2.3 Federal Information Security Modernization Act (2002)

The Federal Information Security Modernization Act (FISMA), first enacted in 2002 and updated in December 2014, established roles and responsibilities for OMB, DHS, and agency CIOs to provide accountability for the delivery of information security capabilities.[177] The 2014 FISMA update simplifies existing reporting to eliminate inefficient or wasteful reporting, while adding new reporting requirements for major information security incidents. FISMA requires the head of each Federal agency to provide information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems. Additionally, FISMA requires agency heads to report on the adequacy and effectiveness of the information security policies, procedures, and practices of their enterprise.[178]

FISMA requires agencies to report the status of their information security programs to OMB and requires Inspectors General (IG) to conduct annual independent assessments of those programs. OMB and DHS collaborate with interagency partners to develop the CIO FISMA metrics, and with IG partners to develop the IG FISMA metrics to facilitate these processes. 0MB also works with the Federal privacy community to develop [SAOP] metrics. These three sets of metrics together provide a comprehensive picture of an agency's cybersecurity and privacy performance.[179]

The legislation also provides DHS with authority to develop and oversee the implementation of binding operational directives to other agencies, in coordination and consistent with OMB policies and practices. FISMA codifies DHS's authority to administer the implementation of information security policies for non-national security Executive Branch systems, including providing technical assistance and deploying technologies to these systems. It also places the federal information security incident center (a function fulfilled by US-CERT[180]) within DHS by law.

2.4 Chief Financial Officers Act (1990)[181]

The CFO Act gave OMB new authority and responsibility for directing federal financial management, modernizing the government's financial management systems, and strengthening financial reporting. The act also created the new position of Deputy Director for Management at OMB, who is to be the government's chief official responsible for financial management. While the CFO Act emphasizes improved financial management, it also charges OMB's Deputy Director for Management with overseeing many of the federal government's general management functions. These functions include information policy, procurement policy, property management, and productivity improvement.

The CFO Act also establishes a new Office of Federal Financial Management in OMB to carry out these governmentwide financial management responsibilities. To head this office, the act establishes the

---

[177] CISA. Federal Information Security Modernization Act. https://www.cisa.gov/federal-information-security-modernization-act

[178] CISA. Fiscal Year 2020 CIO FISMA Metrics. https://www.cisa.gov/sites/default/files/publications/FY%202020%20FISMA%20CIO%20Metrics_v1.pdf

[179] OMB M-20-04. Fiscal Year 2019-2020 Guidance on Federal Information Security and Privacy Management Requirements. 11/19/2019. https://www.whitehouse.gov/wp-content/uploads/2019/11/M-20-04.pdf

[180] CISA. US-CERT. https://us-cert.cisa.gov/

[181] GAO. The Chief Financial Officers Act: a Mandate for Federal Financial Management Reform. September 1991. https://www.gao.gov/special.pubs/af12194.pdf

position of Controller, an individual who is to possess "demonstrated ability and practical experience in accounting, financial management, and financial systems." This individual will handle day-to-day operations to ensure that financial operations are being properly carried out governmentwide.

The 24 CFO Act Agencies include:

- Agency for International Development
- Department of Agriculture
- Department of Commerce
- Department of Defense
- Department of Education
- Department of Energy
- Department of Health and Human Services
- Department of Homeland Security
- Department of Housing and Urban Development
- Department of the Interior
- Department of Justice
- Department of Labor
- Department of State
- Department of Transportation
- Department of the Treasury
- Department of Veterans Affairs
- Environmental Protection Agency
- General Services Administration
- National Aeronautics and Space Administration
- National Science Foundation
- Nuclear Regulatory Commission
- Office of Personnel Management
- Small Business Administration
- Social Security Administration

2.5 Privacy Act (1974)

The Privacy Act[182] establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by Federal agencies. A system of records is defined as a group of records under the control of an agency from which information is retrieved by the name of the individual or by some identifier assigned to the individual.

The Privacy Act requires that agencies give the public notice of their systems of records by publication in the Federal Register. The Privacy Act prohibits the disclosure of a record about an individual from a system of records absent the written consent of the individual, unless the disclosure is pursuant to one

[182] 5 U.S.C. § 552a. Title 5 Government Organizations and Employees. https://www.govinfo.gov/content/pkg/USCODE-2018-title5/pdf/USCODE-2018-title5-partI-chap5-subchapII-sec552a.pdf

of twelve statutory exceptions. The Act also provides individuals with a means by which to seek access to and amendment of their records and sets forth various agency record-keeping requirements.[183]

2.6 Government Performance and Results Act (1993)[184]

The GPRA Modernization Act of 2010 was enacted in January 2011. The Act modernized the Federal Government's performance management framework, retaining and amplifying some aspects of the Government Performance and Results Act of 1993 (GPRA 1993) while also addressing some of its weaknesses. GPRA 1993 established strategic planning, performance planning and performance reporting for agencies to communicate progress in achieving their missions. The GPRA Modernization Act established some important changes to existing requirements. Subsequently, the GPRA Modernization Act of 2010 (GPRAMA) was enacted, which significantly expanded and enhanced the statutory framework for federal performance management.[185] Agencies are required to develop a five-year strategic plan outlining its mission, long-term goals for the agency's major functions, performance measures, and reporting results.

Building on lessons agencies have learned in setting goals and reporting performance, a heightened emphasis is placed on priority-setting, cross-organizational collaboration to achieve shared goals, and the use and analysis of goals and measurement to improve outcomes. The GPRA Modernization Act serves as a foundation for engaging leaders in performance improvement and creating a culture where data and empirical evidence play a greater role in policy, budget and management decisions.

The purposes of the GPRA Modernization Act of 2010 are to:

- Improve the confidence of the American people in the capability of the Federal Government, by systematically holding Federal agencies accountable for achieving program results;
- Improve program performance by requiring agencies to set goals, measure performance against those goals and report publicly on progress;
- Improve Federal program effectiveness and public accountability by promoting a focus on results, service quality and customer satisfaction;
- Help Federal managers improve service delivery, by requiring that they plan for meeting program goals and by providing them with information about program results and service quality;
- Improve congressional decision-making by providing information on achieving statutory objectives and on the relative effectiveness and efficiency of Federal programs and spending; Improve internal management of the Federal Government; and
- Improve usefulness of performance and program information by modernizing public reporting.

[183] 5 U.S.C. § 552a. Privacy Act of 1974. https://www.justice.gov/opcl/privacy-act-1974

[184] OMB Circular A-11. Preparation, Submission, and Execution of the Budget. Section 200.4. https://www.whitehouse.gov/wp-content/uploads/2018/06/a11.pdf

[185] Public Law 111-352. GPRA Modernization Act of 2010. https://www.govinfo.gov/content/pkg/PLAW-111publ352/html/PLAW-111publ352.htm

2.7 Paperwork Reduction Act (1980 and 1995)[186]

The Paperwork Reduction Act (PRA) of 1980 established, within OMB, [OIRA]. It requires the Director of OMB to appoint an Administrator as head of OIRA and makes the Director responsible for any functions delegated to the Administrator about the development and implementation of federal information policies and standards.

The Paperwork Reduction Act (PRA) of 1995 gives OMB authority over the collection of certain information by Federal agencies. It is intended, "among other things, to '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' and to 'improve the quality and use of Federal information to strengthen decision-making, accountability, and openness in Government and society.'"[187] The Act requires agencies to plan for the development of new collections of information and the extension of ongoing collections well in advance of sending an information collection request to OMB. Agencies must:

- Seek public comment on proposed collections of information by placing a notice in the Federal Register;
- Certify to OMB that efforts have been made to reduce the burden of the collection; and
- Review and approve information collection requests internally before submitting them to OMB.

Although the scope of the PRA has changed over the years, its underlying policy standards remain the same. The PRA seeks to:

- Minimize the paperwork burden on the public and other entities;
- 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;
- Improve the quality and use of Federal information to strengthen decision making, accountability, and openness in Government and society;
- Minimize the cost to the Federal Government of creating, collecting, maintaining, using, disseminating, and disposing of information; and
- Ensure the integrity, quality, and utility of the Federal statistical system.[188]

2.8 Government Paperwork Elimination Act (1998)[189]

The Government Paperwork Elimination Act (GPEA) seeks to "preclude agencies or courts from systematically treating electronic documents and signatures less favorably than their paper

[186] 44 U.S.C. Chapter 35. Paperwork Reduction Act of 1980. https://digital.gov/resources/paperwork-reduction-act-44-u-s-c-3501-et-seq/

[187] OMB. Memorandum for the Heads of Executive Departments and Agencies, And Independent Regulatory Agencies. 4/7/2010. http://www.whitehouse.gov/sites/default/files/omb/assets/inforeg/PRAPrimer_04072010.pdf.

[188] OPM. Paperwork Reduction Act (PRA) Guide. 4/27/2011. https://www.opm.gov/about-us/open-government/digital-government-strategy/fitara/paperwork-reduction-act-guide.pdf

[189] OMB. Implementation of the Government Paperwork Elimination Act. https://obamawhitehouse.archives.gov/omb/fedreg_gpea2/

counterparts", so that citizens can interact with the Federal government electronically (S. Rep. 105-335). It requires Federal agencies, by October 21, 2003, to provide individuals or entities that deal with agencies the option to submit information or transact with the agency electronically, and to maintain records electronically, when practicable. It also addresses the matter of private employers being able to use electronic means to store, and file with Federal agencies, information pertaining to their employees. GPEA states that electronic records and their related electronic signatures are not to be denied legal effect, validity, or enforceability merely because they are in electronic form. It also encourages Federal government use of a range of electronic signature alternatives.

2.9 Information Quality Act (2000)[190]

Section 515 of Public Law 106-554, known as the Information Quality Act, required the [OMB] to promulgate guidance to agencies ensuring the quality, objectivity, utility, and integrity of information (including statistical information) disseminated by Federal agencies. OMB's government-wide guidelines, published as interim final on September 28, 2001 (66 F.R. 49718) and finalized on February 22, 2002 (67 F.R. 8452)[191], can be found on [Reginfo.gov]. Federal agencies were also required by Section 515 to publish their own agency specific guidelines no later than one year after OMB's guidelines.

2.10 Freedom of Information Act (2000)[192]

Allows for the full or partial disclosure of previously unreleased information and documents controlled by the United States government. FOIA defines agency records subject to disclosure, outlines mandatory disclosure procedures, and grants exemptions to the statute.

The FOIA provides that when processing requests, agencies should withhold information only if they reasonably foresee that disclosure would harm an interest protected by an exemption, or if disclosure is prohibited by law. Agencies should also consider whether partial disclosure of information is possible whenever they determine that full disclosure is not possible and they should take reasonable steps to segregate and release nonexempt information. The Office of Information Policy at the Department of Justice is responsible for issuing government-wide guidance on the FOIA as part of its responsibilities to encourage all agencies to fully comply with both the letter and the spirit of the FOIA.

[190] OMB. Agency Information Quality Guidelines. https://obamawhitehouse.archives.gov/omb/inforeg_agency_info_quality_links/

[191] Federal Register. Guidelines for Ensuring and Maximizing the Quality, Objectivity, Utility, and Integrity of Information Disseminated by Federal Agencies; Republication. 2/22/2002. https://www.federalregister.gov/documents/2002/02/22/R2-59/guidelines-for-ensuring-and-maximizing-the-quality-objectivity-utility-and-integrity-of-information

[192] DOJ. What is FOIA? https://www.foia.gov/about.html

2.11 Confidential Information Protection and Statistical Efficiency Act (2002)

Enacted to protect the confidentiality of information acquired from the public. The Confidential Information Protection and Statistical Efficiency Act of 2002 (CIPSEA), Title V of the E-Government Act of 2002 (Pub. L. No. 107-347), has two subtitles.[193]

Subtitle A, Confidential Information Protection, concerns confidentiality and statistical uses of information. The purposes of Subtitle A are:

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 title nor have that information used for any purpose other than a statistical purpose; and
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.

CIPSEA Subtitle A protects information that is acquired for exclusively statistical purposes under a pledge of confidentiality. This subtitle of the law applies to all Federal agencies that acquire information under these carefully prescribed conditions. The protection of information collected under this law is supported by a penalty of a Class E Felony for a knowing and willful disclosure of confidential information.

CIPSEA Subtitle B promotes statistical efficiency through limited sharing of business data among three designated statistical agencies, the Bureau of the Census (Census), the Bureau of Economic Analysis (BEA), and the Bureau of Labor Statistics (BLS). The purposes of Subtitle B are:

1. To authorize the sharing of business data among Census, BEA, and BLS 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 Census, BEA, and BLS 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; and
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.

[193] OMB. Implementation Guidance for Title V of the E-Government Act. October 2006. https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/omb/inforeg/proposed_cispea_guidance.pdf

2.12 Digital Accountability and Transparency Act (2014)[194]

Enacted to improve the quality and transparency of Federal award data.

On September 26, 2006, Federal Funding Accountability and Transparency Act (FFATA) was signed into law. The legislation required that federal contract, grant, loan, and other financial assistance awards be displayed on a publicly accessible and searchable website to give the American public access to information on how their tax dollars are being spent. On May 9, 2014, DATA Act was signed into law creating the purpose of the DATA Act Team. The legislation expanded FFATA to:

- Include all direct agency spending and link federal contract, grant, and loan spending to specific agency programs;
- Set government-wide standards for financial data so we can accurately show consistent, reliable, and searchable data;
- Simplify reporting, streamline requirements for reporting, and reduce the cost of complying with the requirements, while improving transparency; and
- Improve the quality of the data at USAspending.gov by holding agencies accountable.

2.13 Geospatial Data Act (2018)

Codifies the Federal Geographic Data Committee and supports the National Spatial Data Infrastructure

The Geospatial Data Act of 2018 (GDA) became law on October 5, 2018. The GDA was included as a component of the FAA Reauthorization Act (P.L. 115-254, Subtitle F). The GDA codifies the committees, processes, and tools used to develop, drive, and manage the National Spatial Data Infrastructure (NSDI) and recognizes responsibilities beyond the Federal government for its development. The GDA reflects growing recognition of the essential role of geospatial data and technology in understanding and managing our world and highlights the need to support their continuing development as critical investments for the Nation.[195]

The GDA reduces duplicative efforts and facilitates the efficient procurement of geospatial expertise, technology, services, and data from the rapidly growing geographic community in the United States. The GDA:

- Aligns business strategies and technology;
- Ensures that resources are managed in accordance with the Nation's needs and priorities; and
- Ensures that all technology resources and employees are utilized in a manner that provides the best value for the Nation

[194] Bureau of the Fiscal Service. About the Data Transparency Program. 6/8/2020. https://fiscal.treasury.gov/data-transparency/history-overview.html

[195] Federal Geographic Data Committee. Geospatial Data Act of 2018. https://www.fgdc.gov/gda/gda-fact-sheet-may-2019.pdf

2.14 Evidence-Based Policy Making Act (2018)[196]

Establishes processes for the federal government to modernize data management practices, evidence-building functions, and statistical efficiency.

The Foundations for Evidence-Based Policymaking Act (or OPEN Government Data Act, Pub.L. 115–435) is a United States law that requires the federal government to modernize its data management practices.

The bill requires agencies to submit annually to [OMB] and Congress a systematic plan for identifying and addressing policy questions. The plan must include, among other things:

- Questions for developing evidence to support policymaking;
- Data the agency intends to collect, use, or acquire to facilitate the use of evidence in policymaking;
- Methods and analytical approaches that may be used to develop evidence to support policymaking; and
- Challenges to developing evidence to support policymaking, including any statutory or other restrictions to accessing relevant data.

Each agency shall designate a senior employee as Evaluation Officer to coordinate evidence-building activities and an official with statistical expertise to advise on statistical policy, techniques, and procedures.

2.15 Open Government Data Act (2018)

Requires public government data assets to be published as machine-readable data, and each agency shall develop and maintain a comprehensive data inventory and designate a Chief Data Officer.

On January 14, 2019, the Open, Public, Electronic and Necessary (OPEN) Government Data Act,[197] as part of the Foundations for Evidence Based Policymaking Act, became law. The OPEN Government Data Act makes Data.gov a requirement in statute, rather than a policy. It requires federal agencies to publish their information online as open data, using standardized, machine-readable data formats, with their metadata included in the Data.gov catalog. Data.gov is working with an expanded group of federal agencies to include their datasets in Data.gov as they implement the new law. In addition, the law requires that GSA work with [OMB] and the Office of Government Information Services to establish an "online repository of tools, best practices, and schema standards to facilitate the adoption of open data practices across the Federal Government." This new repository, which will be an update and expansion of Project Open Data, will also be available on Data.gov.[198]

---

[196] CIO. Foundations for Evidence-Based Policymaking Act of 2018. https://www.cio.gov/policies-and-priorities/evidence-based-policymaking/

[197] Open, Public, Electronic, and Necessary Government Data Act. 3/29/2017. https://www.congress.gov/bill/115th-congress/house-bill/1770

[198] GSA. Data.gov at Ten and the OPEN Government Data Act. 5/31/2019. https://www.data.gov/meta/data-gov-at-ten-and-the-open-government-data-act/

2.16 Creating Advanced Streamlined Electronic Services for Constituents Act (2019)

Enacted in 2019, the Creating Advanced Streamlined Electronic Services for Constituents (CASES) Act directs OMB to require each federal agency to accept electronic identity proofing and authentication processes that allow an individual, under the [Privacy Act of 1974], to access the individual's records or to provide prior written consent for the disclosure of the individual's records.[199] The bill modernizes the way members of Congress receive permission from constituents before contacting federal agencies on their behalf. Instead of a paper submission, constituents who request casework from their congressional representatives every year have the option of submitting a privacy release form electronically.

2.17 Internet of Things Cybersecurity Improvement Act of 2020

Enacted in 2020 to establish minimum security standards for [Internet of Things (IoT)] devices owned and controlled by the federal government. This law gives authority to the CIO to prohibit the head of any agency from "procuring or obtaining, renewing a contract to procure or obtain, or using an [IoT] device" if they find through a mandatory review process that the use of the device prevents compliance with NIST standards and guidelines.

The CIO can waive this requirement only if:

- the waiver is necessary in the interest of national security;
- procuring, obtaining, or using such device is necessary for research purposes; or
- such device is secured using alternative and effective methods appropriate to the function of such device.[200]

2.18 IT Modernization Centers of Excellence Program Act

Enacted in 2020 to establish a program to facilitate the adoption of modern technology by executive agencies. This law codifies the GSA Centers of Excellence (CoEs) Program including the ten existing CoEs and any future ones. It creates a requirement for federal agencies to cooperate on information technology efforts including:

- A commercial cloud computing system that includes
    - end-to-end migration planning and an assessment of progress towards modernization;
    - a cybersecurity and governance framework that promotes industry and government risk management best practice approaches, prioritizing efforts based on risk, impact, and consequences.
- Tools to help an individual receive support from and communicate with an executive agency.
- Contact centers and other related customer supports.

---

[199] Creating Advanced Streamlined Electronic Services for Constituents Act of 2019. https://www.congress.gov/bill/116th-congress/senate-bill/435

[200] Public Law 116-207. IoT CyberSecurity Improvement Act of 2020. https://www.congress.gov/bill/116th-congress/house-bill/1668/text

- Efficient use of data management, analysis, and reporting.
- The optimization of infrastructure, including for data centers, and the reduction of operating costs.
- Artificial intelligence[201]

[201] Public Law 116-194. Information Technology Modernization Centers of Excellence Program Act. https://www.congress.gov/116/plaws/publ194/PLAW-116publ194.pdf

3. Other Authorities

3.1 Executive Orders (EOs)

An EO is a declaration by the president which has the force of law, usually based on existing statutory powers, and requiring no action by the Congress. They are numbered consecutively, so executive orders may be referenced by their assigned number, or their topic. A sitting U.S. President may overturn an existing executive order[202] by issuing another executive order to that effect.[203]

Recent relevant EOs:

- Executive Order 13800 (EO 13800)[204]

3.2 OMB Circulars

An OMB Circular provides instructions or information issued to Federal agencies which are expected to have a continuing effect of two years or more.[205] Circulars are one of the primary ways OMB provides detailed instructions and information to Federal agencies. Importantly, Circulars standardize implementation guidance for Federal agencies across an array of policy areas and topics that are central to the Federal Government's management and budget processes.

Circular A-130:[206]

- In July 2016, [OMB] revised Circular A-130, Managing Information as a Strategic Resource[207], to reflect changes in law and advances in technology. The revisions also ensure consistency with executive orders, presidential directives, recent OMB policy, and National Institute of Standards and Technology standards and guidelines.
- The Circular establishes general policy for information governance, acquisitions, records management, open data, workforce, security, and privacy. It also emphasizes the role of both privacy and security in the Federal information life cycle. Importantly, it represents a shift from viewing security and privacy requirements as compliance exercises to understanding security and privacy as crucial elements of a comprehensive, strategic, and continuous risk-based program at Federal agencies.

---

[202] Federal Register. Executive Orders. All Executive Orders Since 1994. https://www.federalregister.gov/presidential-documents/executive-orders

[203] American Bar Association. What Is an Executive Order? 10/9/2020. https://www.americanbar.org/groups/public_education/publications/teaching-legal-docs/what-is-an-executive-order-/

[204] Executive Order 13800. Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure. 5/11/2017. https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/

[205] OMB. Circulars. https://www.whitehouse.gov/omb/information-for-agencies/circulars/

[206] CIO. Circular A-130 Managing Information As a Strategic Resource. https://www.cio.gov/policies-and-priorities/circular-a-130/

[207] Ibid.

Circular A-11:[208]

- The OMB Circular A-11 is a United States government document issued by the Office of Management and Budget in the form of a written advisory that provides information related to the preparation of the various budgets of agencies of the Federal Government. It is the primary document instructing these agencies in methods, requirements, and terminology for submissions to be reviewed for approval.

3.3 OMB Memoranda

The OMB memoranda provides Federal agencies with instructions and implementation guidance for specific management priorities or legislative requirements. They provide annual updates, such as for FISMA reporting requirements, or have longer term guidance for agency implementation. While some memoranda have built in expiration dates, there have been some examples of previous memoranda being rescinded, such as in M-17-15[209] and M-17-26.[210]

See list of relevant OMB memorandums at https://www.whitehouse.gov/omb/information-for-agencies/memoranda/.

3.4 DHS Binding Operational Directive (BOD)

A BOD is a compulsory direction to executive branch departments and agencies for purposes of safeguarding federal information and information systems.[211] Federal agencies are required to comply with these DHS-developed directives. The Department of Homeland Security (DHS) has the statutory responsibility, in consultation with OMB, to administer the implementation of agency information security policies and practices for information systems, which includes assisting agencies and providing certain government-wide protections. A BOD is a compulsory direction to an agency for purposes of safeguarding Federal information and information systems from a known or reasonably suspected information security threat, vulnerability, or risk in accordance with policies, principles, standards, and guidelines issued by the Director of OMB.[212] As part of that responsibility, DHS is authorized to develop and oversee the implementation of binding operational directives to agencies to implement the policies, principles, standards, and guidance developed by the Director of OMB and requirements of FISMA.

See list of DHS BODs at https://cyber.dhs.gov/directives/.[213]

---

[208] GSA. 2019 Revision to OMB Circular A-11, Part 6: Strengthening the Policy Framework for Improving Program and Service Delivery. 8/14/2019. https://www.performance.gov/a-11-revision/

[209] OMB M-17-15. Rescission of Memoranda Relating to Identity Management. 1/19/2017. https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2017/m-17-15.pdf

[210] OMB M-17-26. Reducing Burden for Federal Agencies by Rescinding and Modifying OMB Memoranda. 6/15/2017. https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2017/M-17-26.pdf

[211] 44 U.S.C. § 3552(b)(l). Title 44 Public Printing and Documents. https://www.govinfo.gov/content/pkg/USCODE-2014-title44/pdf/USCODE-2014-title44-chap35-subchapII-sec3552.pdf

[212] DHS. Binding Operational Directive 18-01. Enhance Email and Web Security. 10/16/2017. https://cyber.dhs.gov/assets/report/bod-18-01.pdf

[213] DHS. Binding Operational Directives. https://cyber.dhs.gov/directives/