05

SECTION

KEY ORGANIZATIONS

5. Key Organizations

5.1 Office of Management & Budget (OMB)

OMB is responsible for overseeing Federal agencies' information technology practices. As a part of this core function, OMB develops and ensures implementation of policies and guidelines that drive enhanced technology performance and budgeting across the Executive Branch. The Federal CIO heads OMB's Office of E-Government and Information Technology (E-Gov), which develops and provides direction in the use of Internet-based technologies. The two major policies and guidelines are FITARA and FISMA.

With FITARA, the Common Baseline was set forth and the role of Agency CIOs was expanded with increased responsibilities through the National Defense Authorization Act for Fiscal Year 2015.[256] Per OMB M-15-14, the specific requirements of FITARA include:

- Agency CIO Authority Enhancements
- Enhanced Transparency and Improved Risk Management in IT Investments
- Portfolio Review
- Federal Data Center Consolidation Initiative
- Expansion of Training and Use of IT Cadres
- Maximizing the Benefit of the Federal Strategic Sourcing Initiative
- Governmentwide Software Purchasing Program[257]

With FISMA, information security requirements were set forth based on NIST compliance documents.[258] FISMA requires annual evaluations of the information security program at each federal agency, which are reviewed by DHS and OMB, and incorporated into an annual report to Congress. FISMA states:

- The Director [OMB] shall oversee agency information security policies and practices, including developing and overseeing the implementation of policies, principles, standards, and guidelines on information security.
- Not later than March 1 of each year, the Director [OMB], in consultation with the Secretary [DHS], shall submit to Congress a report on the effectiveness of information security policies and practices during the preceding year.

Each year, not later than such date established by the Director [OMB], the head of each agency shall submit to the Director [OMB] the results of [their agency's] evaluation required under this section.[259]

---

[256] Public Law 113-291. Sec. 831. National Defense Authorization Act for Fiscal Year 2015. https://www.congress.gov/113/plaws/publ291/PLAW-113publ291.pdf#page=148%5D

[257] OMB M-15-14. Management and Oversight of Federal Information Technology. 6/10/2015. https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2015/m-15-14.pdf

[258] NIST. Federal Information Security Management Act (FISMA) Implementation Project. https://www.nist.gov/programs-projects/federal-information-security-management-act-fisma-implementation-project

[259] CIO Council. CISO Handbook. https://www.cio.gov/assets/resources/CISO_Handbook.pdf

5.2 General Services Administration (GSA)

GSA provides many services to the Federal Government. CIOs should be aware that GSA provides management and administrative support and establishes acquisition vehicles for agencies' use. GSA's information technology acquisition services and offerings are updated along with government-wide policy and are offered through collaboration with DHS, OMB, and other organizations both inside and outside the Federal Government.

GSA collaborates with OMB to sponsor Executive Councils for inter-agency communication and also assist OMB in the development of government-wide policies and guidance.[260]

GSA also has an important role in procuring products and services for the government and administers the Federal Acquisition Service (FAS).[261] The FAS possesses the capability to deliver comprehensive products and services across the government at the best possible value. The continuum of solutions available through FAS include:

- Products and Services
- Technology
- Motor Vehicle Management
- Transportation
- Travel
- Procurement and Online Acquisition Tools

Technology Transformation Services

GSA's Technology Transformation Services (TTS) applies modern methodologies and technologies to improve the lives of the public and public servants. They help agencies make their services more accessible, efficient, and effective with modern applications, platforms, processes, personnel, and software solutions.[262]

Federal Risk and Authorization Management Program (FedRAMP)

FedRAMP is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.[263] The program was established through an OMB Memorandum in December 2011[264] and included the FedRAMP Joint Authorization Board (JAB), which is made up of representatives from DOD, DHS, and GSA. The JAB must authorize any cloud services that will hold federal data. Additionally, GSA established the FedRAMP Program Management Office (PMO) which provides the process for Executive departments and agencies, as well as cloud service providers (CSPs), to adhere to the FedRAMP security authorization requirements created by the JAB.

---

[260] GSA.Shared Solutions and Performance Improvement. https://www.gsa.gov/governmentwide-initiatives/shared-solutions-and-performance-improvement

[261] GSA. Federal Acquisition Service. https://www.gsa.gov/about-us/organization/federal-acquisition-service

[262] GSA. Technology Transformation Services. https://www.gsa.gov/about-us/organization/federal-acquisition-service/technology-transformation-services

[263] FedRAMP. FedRAMP Authorization. https://www.fedramp.gov/about/

[264] FedRAMP. Policy: Security Authorization of Information Systems in Cloud Computing Environments. 12/8/2011. https://www.fedramp.gov/assets/resources/documents/FedRAMP_Policy_Memo.pdf

Per FISMA, agencies must authorize the information systems they use, and these requirements apply to cloud services through FedRAMP. As with FISMA, FedRAMP utilizes the NIST SP 800-53 security controls as a baseline, with additional controls unique to cloud computing. As of September 2020, there have been 200 authorized cloud products through FY19-20, which is up from 100 authorizations between FY13-18.[265]

Information on agency authorization for a cloud service offering (CSO) can be found at FedRAMP.gov.

Data Center and Cloud Optimization Initiative Program Management Office (DCCOI PMO)

The GSA DCCOI PMO[266] helps agencies meet the legislative requirements of FITARA, as well as OMB M-19-19, Update to Data Center Optimization Initiative (DCOI).[267] The DCCOI PMO is OMB's managing partner of the DCOI and manages the Cloud and Infrastructure Community of Practice (C&I CoP), supports Cloud Smart and provides best practices and a procurement guide for cloud technology, and supports Application Rationalization by capturing best practices and case studies and assisting agencies with pilots and ongoing implementation support. CIOs may leverage the C&I CoP's expertise and utilize the DCCOI PMO's capabilities including agency-specific DCOI IDC analysis, Cloud Smart, and Application Rationalization processes.

5.3 Department of Homeland Security (DHS)

The Cybersecurity Information Sharing Act of 2015 gives responsibility to the DHS, Director of National Intelligence (DNI), Department of Defense (DoD) and Department of Justice (DOJ) to "develop procedures to share cybersecurity threat information with private entities, non federal agencies, state, tribal, and local governments, the public, and entities under threats."[268] FISMA 2014 amended FISMA 2002 by "codifying DHS authority" to oversee information security policies for non-national security federal Executive Branch systems.[269]

In accordance with CISA, DHS must establish processes where private sector entities can share information about cybersecurity threats with the Federal Government. DHS manages the delivery and adoption of BODs to federal agencies.

The United States Computer Emergency Readiness Team (US-CERT) works within DHS to prevent cyberthreats and coordinate incident response activities. US-CERT works with federal agencies, private sector, research entities, state and local government and international groups to protect the national technology landscape.[270] The Continuous Diagnostics and Mitigation (CDM) Program "delivers

---

[265] FedRAMP. FedRAMP Reaches 200 Authorizations. 9/17/2020. https://www.fedramp.gov/fedramp-reaches-200-authorizations/

[266] CIO Council. The DCCOI PMO. https://www.cio.gov/about/members-and-leadership/cloud-infrastructure-cop/about-the-DCCOI-PMO/

[267] OMB M-19-19. Update to Data Center Optimization Initiative (DCOI). 6/25/2019. https://www.whitehouse.gov/wp-content/uploads/2019/06/M-19-19-Data-Centers.pdf

[268] S.754 - Cybersecurity Information Sharing Act of 2015. https://www.congress.gov/bill/114th-congress/senate-bill/754

[269] CISA. The Federal Information Security Modernization Act of 2014. https://www.cisa.gov/federal-information-security-modernization-act

[270] US-CERT. Infosheet. https://us-cert.cisa.gov/sites/default/files/publications/infosheet_US-CERT_v2.pdf

automated tools" to federal agencies to build defense against threats to the national technology infrastructure.[271]

Cybersecurity and Infrastructure Security Agency (CISA)
CISA is one of the newest federal agencies, established as an independent operational component of DHS in 2018 through the expansion of DHS's National Protection and Programs Directorate (NPPD). CISA is responsible for the national capacity to defend against cyber-attacks, and CISA works with the federal government to provide cybersecurity tools, incident response services, and assessment capabilities to safeguard ".gov" networks. Additionally, CISA houses the National Risk Management Center (NRMC) which is tasked with planning, analysis, and collaboration to identify and address significant risks to critical infrastructure.

CISA's Cybersecurity Division is the focal point for cybersecurity and related IT systems, and is tasked with seven primary functions:

1. Capability Delivery
2. Threat Hunting
3. Operational Collaboration
4. Vulnerability Management
5. Capacity Building
6. Strategy, Resources & Performance
7. Cyber Defense Education & Training

CISA also maintains a Cyber Resource Hub[272] which includes a range of voluntary cybersecurity assessments that evaluate operational resilience, cybersecurity practices, organizational management of external dependencies, and other key elements of a robust cybersecurity framework. Additional information including Best Practices, case studies, training and exercises, and information about CISA's Annual National Cybersecurity Summits can be found on the CISA.gov website.

Continuous Diagnostic Mitigation (CDM) Program
The CDM Program works under CISA to strengthen the cybersecurity of federal departments and agencies. CDM offers "industry-leading, commercial off-the-shelf (COTS) tools to support technical modernization as threats change." This program meets FISMA mandates and delivers four main objectives: reducing threats at the agency level, increasing visibility into the strengths of federal cybersecurity, improving cybersecurity response capabilities, and streamlining FISMA reporting.

US-CERT
US-CERT works under CISA to prevent cyberthreats and coordinate incident response activities. US-CERT works with federal agencies, private sector, research entities, state and local government and international groups to protect the national technology landscape.[273]

[271] CISA. Continuous Diagnostics and Mitigation (CDM). https://www.cisa.gov/cdm
[272] CISA. Cyber Resource Hub. https://www.cisa.gov/cyber-resource-hub
[273] US-CERT. Infosheet. https://us-cert.cisa.gov/sites/default/files/publications/infosheet_US-CERT_v2.pdf

Core Activities:

- Providing cybersecurity protection to Federal civilian executive branch agencies through intrusion detection and prevention capabilities.
- Developing timely and actionable information for distribution to Federal departments and agencies; state, local, tribal, and territorial (SLTT) governments; critical infrastructure owners and operators; private industry; and international organizations.
- Responding to incidents and analyzing data about emerging cybersecurity threats.
- Collaborating with foreign governments and international entities to enhance the nation's cybersecurity posture.[274]

5.4 National Institute of Standards and Technology (NIST)[275]

A bureau of the Department of Commerce (DOC), NIST provides Federal standards and technical resources on information security that CISOs use to ensure agencies effectively manage risk, and OIG uses to evaluate maturity. OMB and DHS leverage NIST guidance as they develop mandates and initiatives. NIST creates mandatory Federal Information Processing Standards (FIPS) and provides management, operational, and technical security guidelines on a broad range of topics, including incident handling and intrusion detection, the establishment of security control baselines and strong authentication.

- NIST publications are collected online in the Computer Security Resource Center (CSRC). NIST develops standards and guidance through a deliberative process with both Federal and civilian input.
- The Framework for Improving Critical Infrastructure Cybersecurity(referred to as the NIST Cybersecurity Framework)[276] provides a common taxonomy and mechanism for organizations to:
    - Describe their current and target cybersecurity postures,
    - Identify and prioritize opportunities for improvement,
    - Assess progress toward their target, and
    - Communicate among internal and external stakeholders about cybersecurity risk.
- Each agency's OIG considers FIPS and SPs when evaluating the effectiveness of agency information security programs. NIST encourages tailoring of guidance to agency needs. OIG expects those tailoring decisions and associated risk decisions to be reflected in the organization's policies, procedures, and guidance.
- The NIST Risk Management Framework (RMF)[277] provides a foundational process that integrates security and risk management activities into the system development life cycle and brings many of the NIST documents together into an overall approach to managing risk.
- NIST's National Cybersecurity Center of Excellence (NCCoE) is a collaborative hub where industry organizations, Government agencies, and academic institutions work together to address businesses' most pressing cybersecurity issues.

[274] CIO Council. CISO Handbook. https://www.cio.gov/assets/resources/CISO_Handbook.pdf
[275] CIO Council. CISO Handbook. https://www.cio.gov/assets/resources/CISO_Handbook.pdf
[276] USDOC. NIST Cybersecurity Framework. https://www.nist.gov/cyberframework
[277] NIST. FISMA Implementation Project. https://csrc.nist.gov/projects/risk-management/rmf-overview

5.5 Government Accountability Office (GAO)

GAO, headed by the Comptroller General of the United States, is an independent, nonpartisan agency that works for Congress. As part of their mission to investigate how the Federal Government spends taxpayer dollars, they conduct evaluations of agencies' information security policies and practices.[278] The House Committee on Oversight and Reform working with GAO releases a scorecard every six months evaluating federal agencies' implementation of FITARA.[279]

In 2004, GAO recommended to Congress in GAO-04-823 a restructuring of the IT management and reporting responsibilities for the CIO. The GAO identified the full scope of the CIO role and any needed revisions to the Clinger-Cohen Act to increase the efficiency and strength of this title in GAO-11-634. A 2017 GAO forum identified key tasks and actions to strengthen FITARA and enhance the CIO role. In 2018, GAO published a report GAO-18-93 with proposals to OMB and 24 federal agencies to increase CIO efficiency in fulfilling their responsibilities in each of six IT management areas. OMB released FITARA guidance requiring CAOs to accurately inform CIOs of IT contracts for revision and approval. GAO explored in GAO 18-42 the role of CIOs in reviewing and approving IT acquisitions. In the findings, GAO strongly advised federal agencies to "involve the acquisition office in their process to identify IT acquisitions for CIO review, as required by OMB."[280]

GAO Auditing

GAO is an independent, nonpartisan agency that is headed by the Comptroller General and works for Congress and is tasked with examining how taxpayer dollars are spent and providing Congress and federal agencies with objective and reliable information to help the government save money and work more efficiently.[281] One of the GAO's functions is auditing government entities in order to provide essential accountability and transparency over government programs, as well as providing best practices. GAO works with the House Committee on Oversight and Reform to release a scorecard every six months grading federal agencies on their implementation of FITARA. The FITARA scorecard reflects agency performance in eight FITARA-related categories: incremental development, risk reporting, portfolio management, data-center consolidation, software licensing, modernizing government technology, information security management, and CIO reporting structure.[282] GAO's auditing standards can be found in the Yellow Book and GAO provides additional standard-setting guides such as the Financial Audit Manual, Federal Information Systems Controls Audit Manual, and the Standards for Internal Control in the Federal Government, also known as the Green Book.[283] GAO's reports are submitted to Congress and in the reports, GAO will often make recommendations to OMB and agencies. One recent and relevant GAO report is GAO-18-93, [Federal Chief Information Officers: Critical Actions Needed to Address Shortcomings and Challenges in Implementing Responsibilities] which identified

[278] GAO. About GAO - Overview. https://www.gao.gov/about/

[279] House Committee on Oversight and Reform. FITARA 9.0. 12/11/2019 https://oversight.house.gov/legislation/hearings/fitara-90

[280] GAO-18-42. Agencies Need to Involve Chief Information Officers in Reviewing Billions of Dollars in Acquisitions. January 2018. https://www.gao.gov/assets/690/689345.pdf

[281] GAO. About GAO - Overview. https://www.gao.gov/about

[282] House Committee on Oversight and Reform. FITARA 9.0. 12/11/2019 https://oversight.house.gov/legislation/hearings/fitara-90

[283] GAO. About GAO - Role as an Audit Institution. https://www.gao.gov/about/what-gao-does/audit-role/

problems, made recommendations, and helped lead to EO 1388, [Enhancing the Effectiveness of Agency Chief Information Officers].[284]

5.6 Office of the Inspector General (OIG)

The Inspector General Act of 1978 created twelve Offices of Inspector General and by 2019, this number grew to "74 statutory Inspector General's operating in the federal government."[285] Congress passed the IG Act to assign duties to each OIG to investigate and audit programmatic activities, foster efficiency and prevent "fraud and abuse in the programs administered by each agency."[286]

OIG conducts investigations and reviews to oversee the efficiency, effectiveness, financial health and safety of the agencies they serve. FISMA requires each agency's Inspector General (IG) to conduct a yearly independent review of informational security practices. The CIO Council in collaboration with OMB, DHS and the Council of the Inspectors General on Integrity and Efficiency (CIGIE) develops metrics for these evaluations which are updated annually.

5.7 National Archives and Records Administration (NARA)

NARA preserves documents, materials and records involving the Federal Government.[287] NARA collects and maintains declassified information and makes it available for research purposes. In 2019, OMB issued Memorandum M-19-21 providing guidance to all federal agencies to manage records digitally by December 31, 2022, requiring NARA to be accessible in a fully electronic format.[288] This terminated any paper or hard copy systems involving the maintenance of electronic records.

NARA defines essential records as documentation allowing agencies to fulfill their operational needs under a national security threat or emergency, or to safeguard the legal and financial rights of the Federal Government.[289] NARA directs the heads of federal agencies with specific responsibilities in managing essential records including:

- Create and maintain records for the agency;
- Establish programs to manage records to properly identify information for public disclosure and in a digital format, among other standards;
- Transfer of records to record centers;
- Developing protections to prevent loss of records; and
- Notifying Archivist of unlawful activities.

---

[284] GAO-18-93. Critical Actions Needed to Address Shortcomings and Challenges in Implementing Responsibilities. August 2018. https://www.gao.gov/assets/700/693668.pdf

[285] Congressional Research Service. Statutory Inspectors General in the Federal Government: A Primer. 1/3/2019. https://crsreports.congress.gov/product/pdf/R/R45450

[286] H.R.8588 - Inspector General Act of 1978. https://www.congress.gov/bill/95th-congress/house-bill/8588

[287] NARA. About the National Archives. https://www.archives.gov/about

[288] OMB M-19-21. Transition to Electronic Records. 6/28/2019. https://www.archives.gov/files/records-mgmt/policy/m-19-21-transition-to-federal-records.pdf

[289] NARA. Essential Records Guide. August 2018. https://www.archives.gov/files/records-mgmt/essential-records/essential-records-guide.pdf

NARA's Code of Federal Regulations require agencies to establish electronic information systems and evaluate them to check for accuracy. Otherwise, "agencies must submit an SF 115, Request for Records Disposition Authority, to NARA."[290]

[290] 36 C.F.R. §1236.26(a). Electronic Records Management. https://www.ecfr.gov/cgi-bin/text-idx?SID=2cb32d56fb6af59e4b4ee022f092b321&mc=true&node=pt36.3.1236&rgn=div5