MS 129 Office of the Chief Information Officer: Organization, Mission, and Functions

Effective Date: April 29, 2024
Responsible Office: Office of the Chief Information Officer (OCIO)
Supersedes: 04/02/18, 08/25/11; Interim Policy Statement (10/15/97)

Issuance Memo
Issuance Memo (08/25/2011)
Issuance Memo (04/02/2018)
Issuance Memo (04/29/2024)

[Technology Advisory Board Charter](#)

1.0   Authorities

Peace Corps Act, 22 USC 2501, et seq.; Paperwork Reduction Act of 1995, 44 U.S.C. § 3506, as amended by the Information Technology Management Reform Act of 1996; [44 U.S.C. § 3601 Chapter 36 Management and Promotion of Electronic Government Services](#), [Clinger-Cohen Act of 1996](#); Federal Information Security Management Act of 2002 (FISMA), Public Law 107-347, Title III (44 USC 3541 et. seq.); [Office of Management and Budget (OMB) Circular A-130](#)

[Managing Information as a Strategic Resource](#); [Federal Information Technology Acquisition Reform Act of 2014 (FITARA)](#)[1]; [Presidential Memorandum M-18-12 on Implementation of the Modernizing Government Technology (MGT) Act of 2017](#); [OMB Circular A-11 Preparation, Submission, and Execution of the Budget](#); [OMB Memorandum M-15-14 Management and Oversight of Federal Information Technology](#); and OMB IT Budget - Capital Planning Guidance.

2.0   Purpose

The purpose of this Manual Section is to describe the organization, mission, and functions of the Office of the Chief Information Officer (OCIO).

3.0   Organization

OCIO is headed by the Chief Information Officer (CIO), who reports directly to the Deputy Director of the agency. OCIO includes the CIO, the Deputy CIO, and six sub-offices: Administrative Services, Business Services, Customer Support Services, Infrastructure Services, Security and Governance, and Service Strategy and Governance.

4.0   Office Missions

4.1   Office of the Chief Information Officer

The mission of OCIO is to:

(a)   Provide advice and other assistance to the Peace Corps Director and other senior management personnel to ensure that unclassified information technology (IT) is acquired, and information resources are managed in a manner that implements the policies, procedures, and the priorities established by the Peace Corps Director.

(b)   Develop, maintain, and facilitate the implementation of a sound, secure, and integrated enterprise architecture.

(c)   Develop, implement, and maintain an enterprise-wide IT and non-classified information security program.

(d)   Promote the effective, efficient, and compliant design and operation of all major agency information resources management processes, including improvements to work processes.

(e)   Monitor and evaluate the performance of all Peace Corps IT programs and systems.

---

[1] Those U.S. government agencies covered by the Chief Financial Officers Act of 1990 are required to adhere to FITARA. However, OMB strongly recommends that agencies not so covered, including the Peace Corps, nevertheless be guided by FITARA for purposes of improving their ability to deliver on mission and conduct agency business. Therefore, the Peace Corps follows this OMB recommendation and is guided by FITARA.

4.1.1 Administrative Services

The Administrative Services sub-office provides OCIO with information and resources related to its staffing of direct hires and contractors, purchase card procurement and logistics, contract management, and travel.

4.1.2 Business Services

The Business Services sub-office provides OCIO with business process design, professional training and assistance, and software development services to enhance user experience and facilitate streamlined agency cross-collaboration.

4.1.3 Customer Support Services

The Customer Support Services sub-office ensures the delivery of IT customer support services.

4.1.4 Infrastructure Services

The function and purpose of the Infrastructure Services sub-office is to ensure the Peace Corps' global networking and server equipment is monitored, managed, and secured.

4.1.5 Security and Governance

The Security and Governance sub-office safeguards Peace Corps IT systems and assets by implementing best practices in security engineering, incident response, and compliance with federal regulations. In addition, it proactively identifies and mitigates threats and efficiently resolves security incidents to protect the agency's reputation, customers, information, and assets.

4.1.6 Service Strategy and Governance

The Service Strategy and Governance sub-office ensures proper implementation of the governance, strategic planning, and performance management frameworks across OCIO to enable OCIO and the agency to make evidence-based, data-driven, and customer-focused IT business decisions.

5.0 Office Functions

5.1 Office of the Chief Information Officer

OCIO is responsible for oversight and implementation of each of the following:

(a) Improving the management and oversight of IT.

(b) Ensuring that Peace Corps IT systems are secure, efficient, available and accessible, and effective, and that such systems enable the agency to accomplish its mission.

(c) Ensuring the use of federally mandated IT security standards, and industry best practices, and compliance with those standards and practices.

(d) Establishing, implementing, and ensuring compliance with an agency-wide information security program.

(e) Working closely with an integrated team of senior executives with expertise in IT, security, budgeting, acquisition, law, privacy, and human resources to implement appropriate risk management measures.

(f) Modernizing IT infrastructure and improving the delivery of digital services.

(g) Assessing knowledge and skill standards established for agency IT personnel and advising the Peace Corps Director in that regard.

(h) Establishing compliance with applicable standards across Peace Corps IT. In consultation with agency stakeholders, standardizes and organizes IT infrastructure to align with business goals. This process includes the analysis, design, planning, and implementation of IT resources that provide for the successful execution of the Peace Corps' mission.

(i) Implementing the budget-linked capital planning and performance-based management of IT systems throughout the agency.

(j) Ensuring OCIO's IT portfolio is consistent with the agency's strategic plan and goals through a coherent and robust framework of IT strategic plans, practices, and improvement efforts of the IT products and services.

(k) Establishing and maintaining a process to regularly evaluate IT resources supporting each strategic objective of the agency.

(l) Ensuring the effectiveness of the infrastructure framework, computing operations, and support of the agency's global network, telecommunications, hardware, and applications.

(m) Providing appropriate software applications with functionality and information integration across the agency.

(n) Ensuring customers' ability to use IT hardware and software in furtherance of the agency's mission through effective user training and documentation.

(o) Reviewing all cost estimates of IT-related costs and ensuring that all acquisition strategies and plans that include IT adhere to the agency's allocation of appropriated funds.

(p) Reviewing and approving all contract actions or interagency agreements that involve IT in accordance with processes defined in OCIO's governing guidelines, policies, and practices and by the TAB.

(q) Publishing a catalog of pre-approved and licensed software and technology for use by the agency.

(r) Developing and implementing a process that allows for identifying, reviewing, and approving IT system and service requests and providing the necessary resources to meet those needs.

(s) Ensuring that authorized acquisitions meet all security, privacy and management requirements in addition to ensuring that adequate licensing and support is available.

(t) Reviewing all proposed IT procurements to ensure they meet all security, privacy and management requirements in addition to ensuring that adequate licensing and support is available.

(u) Providing input to the Peace Corps enterprise risk management (ERM) program through the development and reporting of metrics which contribute to determining the agency's mission, business process and IT security posture.

5.1.1   Administrative Services

The OCIO function of managing information and resources related to OCIO's human resources (HR) for direct hires and contractors, purchase card procurement and logistics, contract management, and travel.

5.1.2   Business Support Services

The OCIO function of providing business process design and software development services includes activities such as business consulting (process re-engineering, project definition, market research); database management and administration; legacy application maintenance; new application development and software package integration; software testing; and software quality assurance.

5.1.3   Customer Support Services

The OCIO function of managing user IT requests and issues, providing appropriate solutions, and following up to address requests and resolve any issues their users experience. Additionally, providing material support for product adoption and implementation of new technologies being deployed to the agency.

5.1.4   Infrastructure Services

The OCIO function of planning and management of the agency's information and communications technology.

5.1.5   Security and Governance

The OCIO function of assuring IT security and compliance includes all activities under the agency's information security program, including agency cyber security awareness and role based training; conducting systems assessment and authorization; advising on IT security and risk management; testing systems security; assessing agency infrastructure and operations security vulnerability and patch management; monitoring and reporting enterprise information and systems breaches and incidents; and the development of cyber security policy and configurations.

5.1.6   Service Strategy and Governance

The OCIO function of managing agency IT systems, change management, agency records management, strategic planning, performance and execution, service management, and IT portfolio management.

6.0   Effective Date

The effective date of this Manual Section is the date of issuance.