MS 542 Peace Corps IT Security Policies and Procedures

Effective Date: July 19. 2012
Responsible Office: Office of Management/ CIO
Supersedes: 1/26/06; 05/21/02; 06/16/88

Transmittal Memo MS 542
Issuance Memo (07/19/12)

Rules of Behavior - General

Rules of Behavior - Privileged

Table of Contents

1.0 Purpose

This Manual Section sets forth the mandatory security control standards necessary to protect the confidentiality, availability, integrity, authenticity, and non-repudiation of information created, collected, processed, aggregated, transmitted, stored, or disposed of, by or on behalf of Peace Corps information systems and business processes. These control standards are part of the Peace Corps Information Security Program, which is implemented by the Chief Information Security Officer (CISO) under the direction of the Chief Information Officer (CIO) as a part of the Peace Corps OCIO Standards of Practice and Governance.

2.0 Authorities

This Manual Section is based upon federal laws, requirements, and regulations governing information security. This includes the Federal Information Security Management Act of 2002 (FISMA), National Institute of Standards and Technology (NIST) Special Publications, Office of Management and Budget (OMB) Circulars and Memorandums, Federal Information Processing Standards (FIPS) Publications.

3.0 Applicability

This Manual Section applies to the security of all information created, collected, processed, aggregated, transmitted, stored, or disposed of, by or on behalf of Peace Corps. It must be followed by all Peace Corps employees, contract personnel, and Volunteers and Trainees, both domestically and internationally.

4.0 Policy

It is the policy of the Peace Corps to protect Peace Corps information and information systems from unauthorized access, unauthorized changes and unauthorized disruption of service. The Peace Corps Information Security Program is an agency-wide program that protects the information and information systems that support the operations and assets of the Peace Corps. This includes those provided or managed by another agency, contractor, or other source through establishment, dissemination, adherence to and enforcement of OCIO Governance, Standards of Practice, and Standard Operating Procedures.

The Peace Corps implements the Information System Security Program through management, operational and technical controls that provide a framework to protect Peace Corps information and information systems.

(a) Management controls involve those safeguards and countermeasures that manage the security of the information and information systems, and the associated risk to Peace Corps assets and operations. These controls focus on the management of risk. The manner in which these policies and controls are implemented depends on the security categorization level and risks, associated with the specific systems and data involved. In some cases, basic security control policy may need to be modified or supplemented in order to address application-specific or system-specific requirements.

(b) Operational controls support the day-to-day procedures and mechanisms to protect Peace Corps information and information systems. They concern requirements to design, maintain, and use Peace Corps systems in a secure environment. These controls are primarily implemented by people. The manner in which these policies and controls are implemented depends on the security categorization level and risks, associated with the specific systems and data involved. In some cases, basic security control policy may need to be modified or supplemented in order to address application-specific or system-specific requirements.

(c) Technical controls are those security mechanisms employed within an information system's hardware, software, or firmware to protect the system and its information from unauthorized access, use, disclosure, disruption, modification, or destruction. They are used to authorize or restrict the activities of all levels of users within an individual system by employing access based on a least-privileged and need-to-know approach. Technical Controls provide specific guidance on technical procedures used to protect Peace Corps information resources. The manner in which these controls are implemented depends on the security categorization level and risks, associated with the specific systems and data involved. In some cases, basic security policy controls may need

to be modified or supplemented in order to address application-specific or system-specific requirements.

The Peace Corps Security Program implements security controls that address the following areas: Access Control, Awareness and Training, Audit and Accountability, Security Assessment and Authorization, Configuration Management, Contingency Planning, Identification and Authentication, Incident Response, Maintenance, Media Protection, Physical and Environmental Protection, Planning, Personnel Security, Risk Assessment, System and Services Acquisition, System and Communications Protection, System and Information Integrity, and Information Security Program Management.

The CIO has the authority to delegate responsibility within the Office of the Chief Information Office (OCIO) for the development, dissemination, and maintenance of OCIO Governance, Standards of Practice, Standard Operating Procedures and any supplementary guidance or handbooks necessary to implement the policy established in this Manual Section. The CIO will assure that such implementing documents are made available to personnel on the Peace Corps Intranet. Country Directors may issue additional country-specific procedures for information technology, provided they are consistent with this Manual Section.

5.0 Roles and Responsibilities

All individuals with access to Peace Corps facilities, information systems, or information have responsibilities under the Information Technology Security Policy.

5.1 Peace Corps Director

The Director has the overall responsibility to provide information security protections commensurate with the risk and magnitude or impact of harm to organizational operations and assets, individuals, other organizations that may result from unauthorized access, use, disclosure, disruption, modification, or destruction of: (i) information collected or maintained by or on behalf of the Peace Corps; 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.

The Director is responsible for the following duties, in accordance with provisions of NIST and FISMA:

(a) Ensuring that the information security management processes are integrated with strategic and operational planning processes.

(b) Providing information security protections commensurate with this policy, the Peace Corps information security program and federal regulations;

(c) Ensuring that senior Peace Corps officials provide information security for the information and information systems that support the operations and assets under their control;

(d) Ensuring that the Peace Corps has trained personnel sufficient to assist Peace Corps in complying with the requirements of this policy and related IT governance, standards of practice, procedures, and guidelines; and

(e) Ensuring that the CIO, in coordination with other senior Peace Corps officials, reports annually to the Director on the effectiveness of the Peace Corps information security program, including progress of remedial actions.

The Director will establish appropriate accountability for information security and provide active support and oversight of monitoring and improvement for the information security program through the delegation of authority to the Chief Information Officer (ref MS 114).

5.2 Chief Information Officer (CIO)

The CIO is the senior organizational official responsible for information technology assurance and compliance. The CIO is responsible for: (i) designating the CISO; (ii) developing and maintaining information security procedures, guidance and control techniques to address all applicable requirements; (iii) overseeing personnel with significant responsibilities for information security and ensuring that the personnel are adequately trained; (iv) assisting senior organizational officials concerning their security responsibilities; and (v) in coordination with other senior officials, reporting annually to the Director on the overall effectiveness of the organization's information security program, including progress of remedial actions.

5.3 Chief Information Security Officer (CISO)

The Chief Information Security Officer (CISO) is an OCIO official responsible for: (i) carrying out the CIO's security responsibilities under FISMA; and (ii) serving as the primary liaison for the CIO to the authorizing officials, information system owners, common control providers, and information system security officers.

The CISO: (i) possesses professional qualifications, including training and experience required to administer the information security program functions; (ii) maintains information security duties as a primary responsibility; and (iii) heads an office with the mission and resources to assist the organization in achieving more secure information and information systems in accordance with the requirements in FISMA.

The CISO's responsibilities for the Information Security Program include the following activities:

(a) Developing and implementing an information system security training and orientation program in accordance with the requirements of FISMA;

(b) Developing, evaluating and providing information about the Peace Corps information security program, and communicating information security program requirements and concerns to Peace Corps management and personnel;

(c) Maintaining documentation used to establish systems security level designations for all information system security plans within the Peace Corps;

(d) Ensuring that information security risk assessments are developed, reviewed, and implemented for the system security plans process;

(e) Ensuring that system security plans are developed, reviewed, implemented, and revised;

(f) Providing leadership and participating in information security incident response and reporting information security incidents in accordance with reporting procedures developed and implemented by Federal mandates, and Peace Corps;

(g) Mediating and resolving systems security issues that arise between Peace Corps organizations, Peace Corps and other federal organizations, or Peace Corps and states or contractors;

(h) Assuring that Peace Corps Information System Security Officers are appointed and trained;

(i) Assisting Peace Corps Information System Security Officers in developing local systems security; and

(j) Researching state-of-the-art systems security technology and disseminating information material in a timely fashion.

5.4 Authorizing Officials

Authorizing Officials (AOs) are 'A Delegates', with the exception of those who report directly to the Director or the Office of Global Operations, or their designated representatives. The AOs have the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations and assets, individuals, and other organizations. The AOs normally have budgetary oversight for an information system or are responsible for the mission and/or business operations supported by the system. Through the security authorization process, AOs are accountable for the security risks associated with information system operations. AOs coordinate their activities with the CIO, CISO, Information System Owners, Information System Security Officers (ISSO), and other interested parties during the security authorization process. AOs are responsible for ensuring that all activities and functions associated with security authorization, which are delegated to the authorizing official designated representatives, are carried out.

5.5 Information Owner

The information owner is a Peace Corps official with statutory, management, or operational authority for specified information and the responsibility for establishing the policies and procedures governing its generation, collection, processing, dissemination, and disposal. In information-sharing environments, the information owner is responsible for establishing the rules for appropriate use and protection of the subject information (e.g., rules of behavior) and retains that responsibility even when the information is shared with or provided to other organizations.

The owner of the information processed, stored, or transmitted by an information system may or may not be the same as the information system owner. A single information system may contain information from multiple information owners. Information owners provide input to information system owners regarding the security requirements and security controls for the systems where the information is processed, stored, or transmitted.

5.6 Information System Owners

An Information System Owner appointed by an Authorizing Official as the organizational official responsible for the procurement, development, integration, modification, operation, maintenance, and disposal of an information system. An Information System Owner is responsible for addressing the operational interests of the system's user community (i.e., users who require access to the information system to satisfy mission, business, or operational requirements) and for ensuring compliance with information security requirements. In coordination with the Information System Security Officer, the Information System Owner is responsible for the development and maintenance of the security plan and ensures that the system is deployed and operated in accordance with the agreed-upon security controls. Based on guidance from the Authorizing Official, the Information System Owner informs appropriate organizational officials of the need to conduct the security authorization, ensures that the necessary resources are available for the effort, and provides the required information system access, information, and documentation to the security control assessor.

5.7 Information System Security Officer

An Information System Security Officer is appointed by the Information System Owner as the individual responsible for ensuring that the appropriate operational security posture is maintained for an information system. The Information System Security Officer works in close collaboration with the Information System Owner and serves as a principal advisor on all matters, technical and otherwise, involving the security of an information system. The Information System Security Officer has the detailed knowledge and expertise required to manage the security aspects of an information system and, in most organizations, is assigned responsibility for the day-to-day security operations of a system. In close coordination with the Information System Owner, the Information System Security Officer plays an active role in the monitoring of a system and its environment of operation to include developing and updating the security documentation of an information system that may include, but not limited to, a system security plan, managing and controlling changes to the system, and assessing the security impact of those changes.

5.8 General Users

Users are personnel who have access to Peace Corps information and information systems. They are responsible for:

(a) Providing acknowledgement of reviewing, understanding, and accepting the Peace Corps Rules of Behavior (PC-1780).

(b) Adhering to the Peace Corps requirements regarding the use of Peace Corps information technology resources, data, and information systems specific rules of behavior for information systems to which they have been granted access.

(c) Being knowledgeable in, and following, Peace Corps security policies and procedures, as well as related Federal policy contained in the Privacy Act, Freedom of Information Act.

(d) Requesting a formal waiver that includes compensating controls for any Information Technology Security Policy and OCIO Standards of Practice and Governance with which they cannot comply.

(e) Promptly reporting any incident where personally identifiable information or other sensitive agency data in electronic or paper media may have been lost, stolen, or compromised.

(f) Completing required information security and functional training.

5.9 Privileged Users

Privileged users are personnel who have elevated or privileged access to Peace Corps information and information systems. This may include individuals with system administrator, system development, or system engineering responsibilities. In addition to the responsibilities identified for General Users, Privileged Users' responsibilities include:

(a) Developing and implementing the information security requirements throughout the system development life cycle up to and including archiving and disposition requirements;

(b) Verifying that the system security requirements of the information systems to which they have privileged access are being met;

(c) Establishing, maintaining, reviewing, and communicating the security safeguards required for protecting the availability, integrity and confidentiality of information systems based on the information's security characterization;

(d) Planning and implementing the on-going maintenance of the information system, including updates, upgrades, and patches in accordance with the system development life cycle and Information Technology Security Policy and Standards of Practice and Governance;

(e) Adhering to the OCIO Standards of Practice and Governance and Standard Operating Procedures; and

(f) Periodically reviewing and verifying that all users of their systems are authorized and are using the required systems security safeguards, in compliance with the Peace Corps information security Program and all related standards, guidelines, and procedures. Ensuring that any information system changes are approved by the Agency's change control board before implantation.

6.0 Effective Date

The effective date is the date of issuance.