MS 542 Information Security Program

Effective Date: August 3, 2021
Responsible Office: Office of the Chief Information Officer (OCIO)
Supersedes: IPS 1-17 05/18/2018; 06/16/17; MS 542 01/07/13; 07/19/12; 01/26/06; 05/21/02; 06/16/88

Issuance Memo (07/19/2012)
Issuance Memo (01/07/2013)
Issuance Memo (06/16/2017)
Issuance Memo (05/09/2018)
Issuance Memo (08/03/2021)

Attachment
IT Security Resource Center – Requirements, Procedures and Standards

Table of Contents

1.0 Purpose

This policy establishes the Peace Corps Information Security Program (Program) to provide security for unclassified Peace Corps information and information systems, provide overarching direction for information security requirements, and define responsibilities of the Director, Associate Directors (ADs), Regional Directors (RDs), the Chief Information Officer (CIO), the Chief Information Security Office (CISO), Information System Owners (SOs) and other key officials. This policy is the formal, foundational documentation from which all procedures, standards, guidance and other directives will be developed in defining comprehensive and integrated information security requirements that are necessary for the Peace Corps' Information Technology (IT) systems to operate within an acceptable level of risk.

2.0 Authorities

The Federal Information Security Modernization Act (FISMA) of 2014 (Public Law 113-283); the Clinger-Cohen Act of 1996; the Privacy Act of 1974 (5 U.S.C. § 552a), as amended; Public Law No: 113-274, Cybersecurity Enhancement Act of 2014; FIPS 200, Minimum Security Requirements for Federal Information and Information Systems; NIST SP 800-18, Revision 1, Guide for Developing Security Plans for Federal Information Systems; the Records Management Act, 44 U.S.C. 31; Executive Order 13800 "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure;" Office of Management and Budget Circular A-130 "Managing Information as a Strategic Resource;" Binding Operational Directives authorized by Section 3553(b)(2) of Title 44, U.S. Code; Guidance found in the National Institute of Standards and Technology (NIST) information security-related special publications, the Office of Management and Budget circulars and other federal government-wide mandates.

3.0 Applicability

This policy covers all Peace Corps information, information technology, technical services and information systems that may be used to create, store, process or transmit Peace Corps information. This includes information and information systems used, managed or operated by a contractor, another agency or other organization on behalf of the agency. MS 542 applies to all Peace Corps employees, contractors, interns, and all other users of Peace Corps information and information systems supporting the operations and assets of the Peace Corps.

4.0 Policy

a) The security of Peace Corps information and information systems is vital to the success of the Peace Corps' mission. This policy provides the Program with both the responsibility and requisite authority to establish the strategy, requirements, procedures and standards intended to protect all Peace Corps information created, collected, processed, stored, transmitted, disseminated, or disposed of by or on behalf of the agency. This includes Peace Corps information residing in information systems operated by the Peace Corps, its contractors, or other government agencies, in any form or format.

b) This IT security policy requires all Peace Corps federal employees, contractors, and other authorized users of the agency's IT resources, to comply with the security requirements

outlined in this policy. This policy must be properly implemented, enforced, and followed to effectively protect the Peace Corps' IT resources and data. Disciplinary actions may be imposed where individuals and/or systems are determined to be non-compliant or in violation of this policy. A violation of this policy may also result in criminal and civil penalties.

c) Executive Order 13800 requires all federal agencies to use the NIST Cybersecurity Framework (CSF) to manage their agency's cybersecurity risk. To support this mandate, the Peace Corps has adapted this security policy and its primary procedural guides for managing risk to align with the Peace Corps' security procedural guides (based on NIST SP 800-53, Revision 4 security control families)[1]. The security objectives for system resources are to provide assurance of confidentiality, integrity, availability, and accountability by employing security controls to manage cybersecurity risk in accordance with EO 13800 and the CSF.

d) A comprehensive and agency specific CSF will be integrated into business operations at all levels of the agency and across organizational units. In establishing a structured program for the agency's information security, the CSF:

    i) Defines and implements a risk management strategy that:

        i. Establishes and maintains inventories of information systems and the hardware and software that support them;

        ii. Communicates the relationship and importance of information systems to the mission and business functions via Business Impact Assessments;

        iii. Identifies information system and supply chain risks to those systems and business functions, communicates those risks and responds to risk at the information system, mission and strategic levels;

        iv. Provides system level assessments that identify and communicate weaknesses in security controls, internal and external threats, vulnerabilities and the potential likelihood and impact of exploitation of those vulnerabilities;

        v. Establishes Plan of Action & Milestones (POA&M) to plan and track the remediation strategies intended to address weaknesses, threats and vulnerabilities identified;

[1] Although NIST 800-53, Rev. 5 was updated and published on September 23, 2020, with supplemental updates in December 10, 2020 and January 26, 2021, respectively, the corresponding 800-53a Rev.5 is not scheduled for publication until September 2021. Correspondingly, the DOJ CSAM GRC in use at PC is not configured to support Rev. 5 at this time. The CISO will update this policy after publication to reflect Peace Corps' updates to its toolsets to officially begin the Rev. 5 migration.

vi. Provides assurance that specific contracting language, such as security, privacy and records management are included in appropriate contracts to mitigate and monitor risks related to contractor systems and services; and

vii. Creates a centralized, enterprise wide portfolio of risks across the organization.

ii) Defines and implements a configuration management plan that:

i. Establishes a repeatable and accountable change management process and standardized solution delivery framework;

ii. Establishes baseline configurations for hardware and software derived from industry best practice guidance like United States Government Configuration Baseline and Center for Internet Security benchmarks; and

iii. Provides a flaw remediation process that addresses software patching and vulnerability remediation.

iii) Defines and implements an identity & access management strategy that:

i. Provides assignment of risk designations and screening of personnel prior to granting access to Peace Corps information systems;

ii. Establishes and manages records of signed Rules of Behavior (*see* IT Security Resource Center for Rules of Behavior), non-disclosure and acceptable use agreements, as appropriate;

iii. Implements strong authentication mechanisms, like PIV or Level of Assurance 4 credentials, for access to Peace Corps facilities and information systems;

iv. Manages privileged accounts in accordance with the principle of least privilege and separation of duties; and

v. Implements appropriate configuration requirements for remote access connections, to include the use of appropriate cryptography, time outs and monitoring.

iv) Defines and implements data protection and privacy controls that:

i. Protect PII and agency sensitive data, as appropriate;

ii. Attempt to prevent unauthorized data exfiltration;

iii. Implement a data breach response plan; and

iv. Provide privacy awareness training for all staff and role-based training for individuals with privileged access to sensitive data.

v) Defines and implements a security awareness & training program that:

i. Provides security awareness training for all staff and role-based training for individuals with privileged access to information systems; and

ii. Performs an assessment of the skills, knowledge and abilities of its workforce to assess gaps and recommend tailored training no less than biennially.

vi) Defines and implements an information security continuous monitoring strategy that:

i. Establishes a process for continuous assessment and reporting on the effectiveness of security controls; and

ii. Establishes a process for granting or denying system authorization to operate or authorization to use. Systems not authorized for use are subject to shut down and removal.

vii) Defines and implements an incident response capability that:

i. Provides processes, both automated and manual, for detecting and analyzing suspected incidents;

ii. Defines processes for handling suspected or confirmed incidents; and

iii. Shares incident response information with Peace Corps individuals with significant security responsibilities, agency stakeholders, contractors that manage or operate information systems on behalf of the Peace Corps and external stakeholders, like the Cybersecurity and Infrastructure Security Agency.

viii) Defines and implements contingency planning strategies that:

i. Uses the results of Business Impact Analyses to guide contingency planning;

ii. Establishes, communicates and tests Information System Contingency Plans (ISCP);

iii. Integrates ISCPs with other continuity plans, like Disaster Recovery and Continuity of Operations Plans;

iv. Provides system backups, data storage and use of alternate storage and alternate processing sites; and

v. Establishes the planning, communication and performance of recovery activities to stakeholders and executive management teams.

A link to the IT Security Resouce Center, housing all requirements, procedures and standards, including the Rules of Behavior, that support the Information Security Program is attached to this policy. Please note, several of the documents contain sensitive implementation instructions and will be made available on an as-needed basis.

5.0 Definitions

For purposes of this Manual Section, the following definitions shall apply:

a) ***Authorization to Operate (ATO)*** is the official management decision given by the Authorizing Official (AO) to authorize operation of an information system and to explicitly accept the risk to Peace Corps operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls. A Peace Corps granted ATO is based on information provided in a Peace Corps developed information system security plan and security authorization package.

b) ***Authorization to Use (ATU)*** is the official management decision given by an authorizing official to authorize the use of an information system, service, or application based on the information in an existing authorization package generated by another organization, and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of controls in the system, service, or application.

c) ***Availability*** means ensuring timely and reliable access to and use of information.

d) ***Cloud*** refers to IT hardware, software and/or services that run and store data on Internet connected servers that are owned and operated by an external entity.

e) ***Common Control Providers*** are service providers responsible for security controls that are available to multiple systems and programs. An example of a common control is the Office of Safety and Security's background adjudication process. This shared service is a security control that can be inherited in the security plans for multiple information systems.

f) ***Confidentiality*** means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information.

g) ***Continuous Monitoring*** is the process and technology used to detect compliance and risk issues associated with information systems. Continuous monitoring consists of continuous assessments, reporting and authorization of information systems, supported by technology that monitors the environment for vulnerabilities.

h) ***Controls*** (Security Controls) are counter measures established to prevent or minimize the impact of security weaknesses being exploited.

i) ***Cybersecurity Framework (CSF)*** is a policy framework of computer security guidance, developed by NIST, that provides a high level taxonomy of outcomes and a methodology to assess and manage those outcomes.

j) ***Information System*** is a discrete set of information resources, hardware and/or software, owned and operated by or on the behalf of the Peace Corps, which are organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of Peace Corps unclassified information.

k) ***Integrity*** is guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.

l) ***Risk*** is the probability of damage, injury, liability, loss, or any other negative effect that is caused by a threat agent exploiting a technical, procedural, or organizational (i.e., lack of resources or management oversight) weakness or vulnerability.

m) ***Risk Management*** is the process of managing risks to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the United States resulting from the operation of an information system. This includes assessing unclassified information system risks, implementing risk mitigation strategy, and employing continuous monitoring to consistently assess the security state of the information system.

n) ***Security Incident*** refers to an event that may cause or result in a loss in the confidentiality, integrity or availability of Peace Corps data or information systems.

6.0 Roles and Responsibilities

The roles and responsibilities described in the paragraphs below are assigned to the offices and positions identified to ensure effective implementation and management of the Program. The establishment of a security management structure and assignment of security responsibilities is a requirement of FISMA. Additional roles are identified and defined in supporting procedures, as needed.

Any re-delegation of an assigned responsibility shall be documented by memorandum and communicated to the CISO or assigned Information System Security Officer (ISSO).

6.1 Peace Corps Director

The Director is responsible for:

a) Ensuring that an agency-wide information security program is developed, documented, implemented, and maintained to protect information and information systems;

b) Ensuring that information security management processes are integrated with agency strategic and operational planning processes;

c) Ensuring that ADs, RDs and other key officials (e.g., Deputies, Division Directors and Office Directors) provide security for the information and information systems that support operations and assets under their control;

d) Ensuring enforcement and compliance with FISMA and related information security directives;

e) Delegating to the CIO the authority for development and implementation of an agency-wide information security program that ensures compliance with FISMA and related information security directives;

f) Ensuring the Peace Corps has trained personnel to adequately assist in complying with FISMA and other related security directives;

g) Ensuring that each IT system, whether government or government contractor operated, undergoes regular security control assessments; and

h) Designating a CISO whose primary duty is development, implementation and oversight of the Peace Corps' Program in support of this policy and relevant information security laws, Executive Branch policy and other directives.

6.2 Authorizing Official (AO)

The AO has the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations, assets or individuals. Through the security authorization process, the AO is accountable for the security risks posed to the information system, interconnected information systems and agency operations that rely on those systems. Accordingly, the AO is in a management position with a level of authority commensurate with understanding and accepting such information system-related security risks. At Peace Corps, this role and its responsibilities are assigned to the CIO. The AO cannot also be the SO for a system operating under his/her authority.

The AO is responsible for:

a) Completing role-based security training prior to executing any signatory responsibilities as the AO;

b) Approving or denying authorization to operate (ATO) or authorization to use (ATU) for an information system. If the system is operational, the AO may halt operations when unacceptable risks exist;

c) Coordinating risk-based analysis activities with the risk executive (function), CISO, SOs, Information System Security Managers, security control assessors, and other stakeholders;

d) Approving and documenting the assignment of personnel to the role of SOs, and ISSOs;

e) Drafting, approving, and reviewing risk acceptance memorandums. Risk acceptance memorandums are temporary exceptions to Peace Corps information security policies, procedures and/or standards. *See* the IT Security Resource Center for all requirements, procedures and standards that support the Program; and

f) Reviewing continuous monitoring reports/dashboard and making a risk-based determination on a system's ongoing authorization status.

6.3 Chief Information Officer (CIO)

The CIO is responsible for:

a) Ensuring the Peace Corps' Program and information security protection measures are compliant with FISMA and related information security directives;

b) Developing, documenting, implementing and maintaining an agency-wide Program as required by this policy, FISMA and related information security directives, that both enables the Peace Corps to meet, and ensures that the Peace Corps does meet, federal information security requirements;

c) Developing, maintaining and issuing agency-wide information security policies, procedures and control techniques to provide direction for implementing the requirements of the Program;

d) Ensuring that personnel with significant information security responsibilities are provided training on the proper execution of such responsibilities. Those individuals include but are not limited to: the Privacy, Records Management, FOIA and Continuity of Operations Officers and others whose activities or duties involve information security responsibilities and are externally managed;

e) Assisting senior agency and other key officials to understand their information security responsibilities and with the implementation of such responsibilities;

f) Establishing minimum, mandatory, risk-based technical, operational and management information security control requirements for agency information and information systems;

g) Reporting any compliance failure or policy violation directly to the appropriate AD, RD or other key official(s) for appropriate disciplinary and corrective action;

h) Requiring any AD, RD or other key official (e.g., Deputies, Division Directors and Office Directors) to report back to the CIO regarding what actions will be taken in response to any compliance failure or policy violation reported by the CIO;

i) Ensuring SOs and ISSOs comply with all Program requirements, including training, and that they have all necessary authority and means to direct full compliance with such requirements;

j) Establishing the Rules of Behavior for appropriate use and protection of the information and information systems supporting the Peace Corps' mission and functions;

k) Developing, implementing and maintaining capabilities for detecting, reporting and responding to information security incidents;

l) Designating a CISO whose primary duty is information security who can carry out the duties and responsibilities of development, implementation and oversight of the Peace Corps' Program in support of this policy and adhere to relevant information security laws, Executive Branch policy and other directives;

m) Ensuring that the CISO heads an office with the mission and the resources required to administer the Program functions, carry out the CIO responsibilities under this policy and assist in ensuring agency compliance with this policy; and

n) Reporting monthly to the Director on the effectiveness of the Program, including progress made on all remedial actions.

6.4 Chief Information Security Officer (CISO)

The CISO is an OCIO official responsible for: (i) carrying out the CIO's security responsibilities under FISMA; and (ii) serving as the primary liaison to SO, common control providers, and ISSOs for the CIO on matters related to Peace Corps' Program and unclassified information security policies and procedures.

The CISO:

a) Develops, documents, and implements an agency-wide IT security program to provide information security for the information and information systems that support the operations and assets of the agency in the most cost-effective manner;

b) Ensures departments are informed on the total cost of ownership requirements required to support this Directive in a timely manner to support resource justifications;

c) Develops and maintains information security policies, procedures, and control techniques to address all applicable requirements for protecting Peace Corps information and information systems;

d) Assists senior Peace Corps officials in performing their information security responsibilities;

e) Develops, maintains, authorizes, and manages a Peace Corps information system risk management framework;

f) Manages the Enterprise Common Controls and associated organizationally defined parameters on behalf of the agency;

g) Reviews and approves cybersecurity policy deviations in consultation and agreement with the AO, where appropriate; and

h) Provides mandatory computer security training for Peace Corps employees and contractors, at the time of hiring/onboarding and on an annual basis, to make them aware of the policies and procedures for protecting sensitive information.

6.5 Associate Directors (ADs), Regional Directors (RDs) and Other Key Officials

ADs, RDs, and other key officials (e.g., Deputies, Division Directors and Office Directors) are responsible for:

a) Implementing the policies, procedures, control techniques and other countermeasures promulgated under the information security program;

b) Complying with FISMA and other related information security laws and requirements in accordance with CIO directives in the execution of appropriate security controls;

c) Ensuring that all employees within their organizations take immediate action to comply with directives from the CIO to (a) mitigate the impact of any potential information security risk, or (b) respond to an information security incident;

d) Ensuring their organizational managers have all necessary authority and means to direct full compliance with directives from the CIO;

e) Enforcing and ensuring the Rules of Behavior and additional rules of behavior for particular systems. If established, these rules are annually signed or acknowledged electronically or manually by all information users and information system users that support the operations and assets of the Peace Corps; and

f) Oversight of SOs within their office, ensuring prompt closure of POA&Ms or needed security remediation efforts to ensure that the security of the systems within their offices are properly maintained and timely with corrective actions.

6.6 System Owners (SOs)

SOs are officials within the Peace Corps who bear the responsibility for the acquisition, development, maintenance, implementation, and operation of the Peace Corps' IT systems. SOs represent the interests of the system throughout its lifecycle. Primary responsibility for managing risk within an information system rests with the SOs. Although the SO bears this responsibility, the technical expertise that supports implementation of the information security requirements is

primarily provided by the ISSO, subject matter experts and system administrators. SOs are responsible for:

a) Following the requirements defined in support of the agency information security program in consultation and coordination with the CIO, CISO, ISSOs, other SOs and subject matter experts (SMEs) throughout the information system's lifecycle;

b) Developing, maintaining and providing information security documents as required for the assigned system;

c) Coordinating with ISSOs and SMEs to decide who has access (and with what types of privileges or access rights) and ensuring system users and support personnel receive the requisite security training for the assigned system;

d) Taking role-based training annually; and

e) Obtaining ATO, ATU or test, from the AO prior to operational use or testing of any system.

6.7 Information System Security Manager (ISSM)

The ISSM directly reports to the CISO and is responsible for:

a) Advising the AO and CISO on information system risk levels and security posture;

b) Advising the AO and CISO on changes affecting the organization's cybersecurity posture;

c) Providing programmatic coordination of information security resources;

d) Coordinating with ISSOs to assure successful implementation and functionality of security requirements and appropriate IT policies and procedures that are consistent with the organization's mission and goals;

e) Coordinating with ISSOs to ensure that remediation plans are defined and documented that adequately address system vulnerabilities, and monitoring their progress until evidence of completion has been provided;

f) Collecting and maintaining data needed to support cybersecurity reporting metrics; and

g) Interpreting patterns of noncompliance to determine their impact on levels of risk and/or overall effectiveness of the enterprise's cybersecurity program.

6.8 Information System Security Officers (ISSO)

ISSOs are responsible for:

a) Supporting the SO and AO in the management and implementation of policies and procedures identified in the Program and ensuring protective measures are compliant

with FISMA and related information security directives for the information, information system and service assigned;

b) Serving as a principal advisor on all matters, technical and otherwise, involving the security of the information, information system or service assigned and for ensuring implementation of adequate system security in order to prevent, detect and recover from security breaches;

c) Coordinating with SOs, contracting officers and SMEs to communicate information security requirements, appropriate controls and user access, and to monitor, test and evaluate the proper implementation, operation and maintenance of the security controls; and

d) Coordinating and acting as a liaison with the Peace Corps and external personnel for system and security management, operations and control monitoring, audits, assessments, incident response and law enforcement.

6.9 Contracting Officers (COs) and Staff with Procurement Authority

COs and staff with procurement authority are responsible for ensuring that all information technology requirements are cleared with the CIO to ensure agency contracts and procurements are compliant with the agency's information security policy and in alignment with the enterprise IT architecture. COs and staff with procurement authority are tasked with ensuring that the appropriate security, privacy and records management-related contracting language is incorporated in each contract and task order and delivered, as required.

6.10 Common Control Providers

Implementation of the agency's information security program depends upon services and responsibilities provided by offices beyond the OCIO. These non-IT services, like asset management, physical security, workforce planning, personnel security, privacy and records management are shared, or common, security controls provided by offices like Safety & Security, Management, Human Resources and Office of the Chief Financial Officer. Common Control Providers are responsible for:

a) Development of the policies and procedures that define their service(s);

b) Management and delivery of those services; and

c) Defining the responsibilities of information systems and programs that utilize those services.

6.11 Office of Inspector General (OIG)

The OIG is responsible for:

a) Conducting an annual review to assess the effectiveness of the security controls and practices of the Program;

b) Reporting annual review results to the Director, Congress and other stakeholders as required, in accordance with the Inspector General Act of 1978, as amended; and

c) Providing independent oversight over information security operations.

6.12 Users

Peace Corps information and information system users (i.e., employees, contractors, interns, Volunteers, and others) supporting the operations or using the assets of the Peace Corps (Users) are responsible for:

a) Complying with all agency information security policies, procedures and other directives;

b) Successfully completing information security awareness training within 30 days of initial access to Peace Corps systems and at least annually thereafter to maintain access;

c) Immediately reporting all suspected information security incidents to IT Security;

d) Signing or acknowledging electronically or manually, at least annually in order to maintain access to Peace Corps systems and information, that they have read, understand and agree to abide by the Rules of Behavior and any additional system-specific rules of behavior, if established prior to their initial access to Peace Corps systems and information;

e) Ensuring that their credentials are not shared with or used by any other person;

f) Ensuring that access to Peace Corps information systems or roles assigned within those systems is the minimum required to perform tasks associated with an assigned role; and

g) Successful completion of information security role-based training prior to initial access to Peace Corps systems by individuals in their designated role(s) and, at least annually thereafter, to maintain access, if the individual is designated as having significant information security responsibilities.

7.0 Policy Exceptions

Requests for exceptions to established policy, procedures or standards established in support of the Program must be submitted in writing and approved by the CISO and AO for a pre-determined period. The CISO, may grant an exception with respect to individual requirements specified in this Manual Section or in guidance only if the system is technically unable to implement the requirement or there is an approved business justification and sufficient compensating controls have been implemented to reduce risk to an acceptable level. At the expiration of any period for which an exception is approved, the exception will be rescinded and obligations for compliance with the original established policy, procedure or standard will be immediately reinstated.

8.0 Effective Date

The effective date is the date of issuance.