MS 550 Cybersecurity Incident Response Program

Effective Date: July 29, 2024
Responsible Office: Office of the Chief Information Officer/Security and Governance (OCIO/SG)

Issuance Memo (07/29/2024)

Table of Contents

1.0 Purpose

The purposes of this policy establishing a Peace Corps Cybersecurity (Cyber) Incident Response Program are to: (i) provide information security for unclassified Peace Corps information and information technology (IT) systems; (ii) provide overarching direction for the implementation of Cyber Incident reporting; and (iii) define the roles and responsibilities within the Cyber Incident Response Program of the Chief Information Officer (CIO), the Chief Information Security Officer (CISO), the Office of Management (OM), and other key agency stakeholders.

This policy provides direction for the development at the agency of all Cyber Incident Response Program procedures, standards, guidance, and other directives that are developed to define the comprehensive and integrated information security requirements necessary for the operation of the Peace Corps' IT systems within an acceptable level of risk.

2.0 Authorities

The Cyber Incident Response principles and practices described in this policy derive their authority from, and are based on, guidance from the National Institute of Standards and Technology (NIST), including NIST Special Publication (SP) 800-61 Revision 2, "Computer Security Incident Handling Guide," and NIST SP 800-53 Revision 5, "Security and Privacy Controls for Information Systems and Organizations;" the Cybersecurity and Infrastructure Security Agency (CISA) Federal Government Cybersecurity Incident and Vulnerability Response Playbooks; the updated CISA Federal Incident Notification Guidelines; and Executive Order (E.O.) 14028, "Improving the Nation's Cybersecurity." E.O. 14028 and the CISA Federal Government Cybersecurity Incident and Vulnerability Response Playbooks provide federal civilian agencies with a standard set of procedures to respond to vulnerabilities and incidents impacting federal civilian executive branch networks. Additional authorities include 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; E.O. 13800, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure;" Office of Management and Budget (OMB) Circular A-130, "Managing Information as a Strategic Resource;" Binding Operational Directives authorized by Section 3553(b)(2) of Title 44, U.S. Code; and other relevant OMB circulars and federal government-wide mandates.

3.0 Scope and Applicability

This policy applies to all IT systems operated by or on behalf of the Peace Corps and its offices in the United States and overseas.

4.0 Definitions

These definitions are derived from the various authorities referred to in subsection 2.0 above.

(a) ***Adverse Events*** are "Events," as defined below, having a negative consequence, such as a system crash, unauthorized use of system privileges, unauthorized access to sensitive data, and executions of malware that destroy data.

(b) An ***Authorized User*** is an individual or (system) process authorized to access an IT system.

(c) ***Breach*** means the loss of control, compromise of, unauthorized disclosure of, and unauthorized acquisition of data or information or unauthorized access to data or information, or any similar occurrence where (1) a person other than an Authorized User accesses or potentially accesses Personally Identifiable Information (PII) or (2) an Authorized User accesses or potentially accesses PII for any purpose other than an authorized purpose.

(d) ***Computer Security Incident or Cyber Incident****,* as defined in NIST Special Publication 800-61, is a violation or imminent threat of violation of computer security policies, information security or privacy policies, acceptable use policies, or standard security practices. A Cyber Incident includes, but is not limited to:

(1) The loss or theft of data or information involving data or information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information linked to a specific individual (i.e., PII);

(2) The transfer of data or information to those who are not entitled to receive that information;

(3) Obtaining sensitive data through an "IT System Attack," as defined below, which poses a threat that the data may be released publicly if the agency does not pay a designated sum;

(4) Attempts (either failed or successful) to gain unauthorized access to data, information storage, or a computer system;

(5) Provision by, or exposure of, sensitive information to unauthorized individuals through peer-to-peer file sharing services; and

(6) Changes to information, data, or system hardware, firmware, or software characteristics without the Authorized User's knowledge, instruction, or consent.

(e) ***Cyber Incident Response Capability*** allows for a systematic agency response (i.e., provides for a consistent incident handling methodology) to Cyber Incidents so that appropriate actions are taken. Development of this capability helps personnel to minimize loss or theft of information and disruption of services caused by Cyber Incidents involving information security.

(f) A ***Cyber Incident Response Plan*** establishes procedures to address IT System Attacks, as defined below. These procedures are designed to enable security personnel to identify, mitigate, and recover from malicious Computer Security Incidents.

(g) ***Event*** is any observable occurrence in an IT system or network. Events include a user connecting to a file share, a server receiving a request for a web page, a user sending email, and a firewall blocking a connection attempt.

(h) ***IT System Attack*** is an occurrence that compromises personal and business data, which must be responded to quickly and effectively to minimize security breaches.

(i) ***IT System Components*** include critical infrastructure IT systems, devices that provide centralized storage capabilities (e.g., desktops, laptops), and other devices that provide distributed computing capabilities, networking devices, and other security devices dedicated to providing security capabilities supporting the Peace Corps mission.

(j) ***Necessary and Appropriate Actions*** are coordinated management decisions or other measures, both precautionary and reactive, undertaken to address, for example, known or suspected Computer Security Incidents, Adverse Events, and significant IT vulnerabilities.

(k) ***Recovery Effort*** is the need to develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a Computer Security Incident.

(l) ***Security Incident Response Team (SIRT)*** is a hybrid team consisting of Incident Response experts within OCIO and outsourced monitoring capability responsible for providing continuous monitoring and detection services for domestic and overseas locations to assist and respond to Computer Security Incidents.

5.0 Policy

(a) The Peace Corps shall establish and maintain Cyber Incident Response Capability to respond to computer or network-based Cyber Incidents to preserve its ability to perform necessary governmental functions, protect the Peace Corps' information and IT system assets, and maintain the confidentiality and integrity of business and personal information in the possession and under the control of the Peace Corps.
A strong Cyber Incident Response Capability depends upon a defined Cyber Incident Response Plan that adheres to each of the following steps:

(1) Prepare for future responses to Cyber Incidents by establishing assets and capabilities to respond to Cyber Incidents and ensuring that all IT systems and IT System Components are sufficiently secure.

(2) Detect Cyber Incidents and analyze their operational and technical impact on the Peace Corps' IT systems, IT System Components, and supported missions.

(3) Contain Cyber Incidents to prevent further damage to the Peace Corps' IT systems, IT System Components, and supported missions.

(4) Remediate, mitigate, or eliminate Cyber Incidents in the Peace Corps' IT systems, IT System Components, and supported missions.

(5) Recover impacted Peace Corps IT systems and Information System Components.

(6) Undertake post-Cyber Incident activities to prevent or lessen the impact of future Cyber Incidents.

(b) To facilitate the Cyber Incident Response Program, responsibility will be assigned to a SIRT. If a Cyber Incident occurs, the members of the SIRT will be charged with executing the Cyber Incident Response Plan. To ensure that the team is fully prepared to undertake its responsibilities, all team members will be trained in Cyber Incident response operations on an annual basis.

(c) Incident Response Plans will be reviewed and, where applicable, revised on an annual basis. The reviews will be based upon the documented results of previously conducted tests or live executions of the Cyber Incident Response Plan. Upon completion of a revision, the updated Cyber Incident Response Plan will be distributed to staff involved in responding to Cyber Incidents.

(d) Cyber Incident response training relevant to assigned roles and responsibilities, shall be provided before access to IT systems or performance of assigned duties may be authorized. Such training shall be provided annually or more frequently as required by IT system changes. The agency shall test the Cyber Incident Response Capability for the IT systems they support at least annually.

6.0 Roles and Responsibilities

6.1 Staff and Volunteer/Trainee Responsibilities

In support of the SIRT, all agency staff, including contractors, and Volunteers/Trainees shall be aware of what constitutes a Cyber Incident and understand the following reporting procedures:

(a) A Breach, whether suspected or confirmed, involving PII in electronic or physical form shall be reported via the IT Service Desk by the person discovering the breach as soon as practicable after discovery.

(1) Whenever there is a suspected or confirmed Breach domestically, any individual who suspects or knows of the Breach shall promptly notify the IT Service Desk by calling +1 202-692-1000 or +1 855-855-1961 and select “Option 5” for IT Support.

(2) When there is a suspected or confirmed Breach overseas, any individual who suspects or knows of the Breach, shall promptly notify the Post IT Specialist. The Post IT Specialist shall then promptly notify the IT Service Desk by calling +1 202-692-1000 or, if a phone is not available, emailing PCHelpDeskSupport@peacecorps.gov.

6.2 Chief Information Officer (CIO)

The CIO is responsible for:

(a) Acting as a conduit to Associate Directors (ADs), Regional Directors (RDs), and other key officials during a suspected or confirmed Cyber Incident;

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

(c) Establishing, implementing, and ensuring compliance with an agency-wide information security program as set forth in MS 542 *Information Security Program*.

6.3 Chief Information Security Officer (CISO)

The CISO is responsible for serving as the Cyber Incident Response Coordinator and may delegate aspects of this function as necessary. These responsibilities include:

(a) Serving as the designated authority for the security operation of agency IT resources;

(b) Taking Necessary and Appropriate Action(s) in response to an actual, suspected, or threatened Computer Security Incident or Significant IT Vulnerability;

(c) Coordinating with other agency offices and security officials within the agency to carry out Necessary and Appropriate Actions;

(d) Providing overall direction to a SIRT;

(e) Overseeing the creation, implementation, and maintenance of a Cyber Incident Response Plan that is consistent with this policy and the following:

(1) E.O. 14028, "Improving the Nation's Cybersecurity,"

(2) CISA Federal Government Cybersecurity Incident and Vulnerability Response Playbooks, and

(3) The NIST cybersecurity framework;

(f) Ensuring mandatory reporting requirements are met whenever a confirmed or suspected Cyber Incident is reported to internal/external stakeholders, including required reporting to the Office of Inspector General (OIG), the Office of the General Counsel (OGC), and OM; and

(g) Ensuring all follow-up reporting to CISA is completed in accordance with CISA Federal Incident Notification Guidelines.

6.4 Security Incident Response Team (SIRT)

The SIRT shall:

(a) Respond to Cyber Incidents or new threats to IT systems or data in accordance with the Cyber Incident Response Plan;

(b) Promptly report Cyber Incident information to appropriate authorities in accordance with the agency's Cyber Incident Response Plan and CISA reporting procedures;

(c) Determine Cyber Incident severity and escalate as appropriate, in consultation with the CISO;

(d) Conduct preliminary assessments to determine root cause, source, nature, and the extent of damage caused by a suspected Cyber Incident;

(e) Maintain confidentiality of information related to Cyber Incidents, providing such information solely on a need-to-know basis;

(f) Assist with Recovery Efforts and provide reports to the CISO;

(g) Document all Cyber Incidents and, as appropriate, include root cause analysis and lessons learned;

(h) Maintain awareness of and implement procedures for an effective response to Cyber Incidents;

(i) Stay current on functional and security operations technologies as these relate to individual's areas of responsibility and expertise; and

(j) Receive annual training on new cyber threats, trends, and best practices.

6.5 Senior Agency Official for Privacy (SAOP)

The SAOP within OM is responsible for:

(a) Responding to a Breach in accordance with MS 899 *Breach Notification Response Plan*;

(b) Participating in all phases of the Peace Corps' planning, preparation, investigation, and response to Breaches involving PII and "Covered Information," as those terms are defined in MS 899; and

(c) Whenever a Breach occurs, coordinating and working with the Office of Safety and Security and the CISO, to ensure that necessary steps are taken to contain and control the Breach and prevent further unauthorized access to or use of PII, which may include changing locks, deactivating facility access cards, enhancing physical security measures, alerting the Federal Protective Service, and/or developing or implementing special instructions, reminders, or training.

6.6 Office of the General Counsel

The Office of the General Counsel is responsible for providing all legal support and guidance associated with any agency responses to a suspected or confirmed Breach.

6.7 Reporting to Law Enforcement, the Office of Inspector General, and the Office of the General Counsel

In accordance with OMB Circular M 17-12, "Preparing for and Responding to a Breach of Personally Identifiable Information," Section VII (D)(2) and the agency's Cyber Incident

Response Plan, the CISO or designee is responsible for notifying and consulting with law enforcement, the Office of Inspector General, and OGC.

7.0 External Reporting Responsibilities

The CISO, or a point of contact designated by the CISO, is responsible for all communications regarding confirmed or suspected Cyber Incidents, including coordination with CISA and other U.S. agencies and departments. The CISO will also notify and coordinate, as necessary, with other Peace Corps officials. The CISO will review and approve the submission of the Peace Corps Cyber Incident reporting information to CISA in accordance with United States Computer Emergency Readiness Team (U.S. CERT) guidelines, as necessary. Potentially sensitive information, PII, or information protected under the Privacy Act related to individuals reporting, involved in, or affected by a Cyber Incident may be redacted from communications or reports.

8.0 Incident Response for PII

Cyber Incidents involving PII that are not "major incidents" generally follow the same process and involve the mitigation activities set forth in this Manual Section but include escalation as soon as practicable to the SAOP as soon as potential PII is found to be at risk, in accordance with CISA guidelines.

9.0 Effective Date

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