MS 405 Classified National Security Information

Effective Date: November 24, 2020
Responsible Office: Office of Safety and Security
Supersedes: 01/07/13; 06/23/11

Issuance Memo (06/23/2011)
Issuance Memo (01/07/2013)
Issuance Memo (11/24/2020)

Table of Contents

1.0 Purpose
2.0 Authorities
3.0 Policy
4.0 Applicability
5.0 Definitions
6.0 Responsibilities
  6.1 Peace Corps Director
  6.2 Associate Director for Safety and Security
  6.3 Chief, Information and Personnel Security Division
  6.4 Chief, Emergency Management and Physical Security Division
  6.5 Employees
7.0 Requirements for Access to Classified National Security Information
  7.1 Determination of Need for Access
  7.2 Access to Classified National Security Information
8.0 Control of Classified National Security Information in Peace Corps Facilities
  8.1 Annual Reviews and Inspections
9.0 Original Classification Authority and Derivative Classification
10.0 Infraction and Violation Program
11.0 Reporting to Information and Security Oversight Office
12.0 Effective Date

1.0 Purpose

The purpose of this Manual Section is to set forth Peace Corps policy for the control and safeguarding of Classified National Security Information.

2.0 Authorities

Executive Order 13526 and 32 CFR Parts 2001 and 2003

3.0 Policy

It is the policy of the Peace Corps to safeguard Classified National Security Information in accordance with Federal directives and laws and that Access to such information will only be given to persons who have a security clearance and valid Need-to-know.

4.0 Applicability

This Manual Section applies to all Peace Corps employees (including personal services contractors) who hold security clearances and are authorized to have access to Classified National Security Information.

5.0 Definitions

(a) ***Access*** is the ability and opportunity to obtain knowledge of classified information. An individual is considered to have had Access by being in a place where national security information is kept, processed, handled, or discussed, if the security control measures that are in force do not prevent the person from gaining knowledge of such information.

(b) ***Classification*** means the act or process by which information is determined to be classified information.

(1) ***"Top Secret"*** shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security that the Original Classification Authority is able to identify or describe.

(2) ***"Secret"*** shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security that the Original Classification Authority is able to identify or describe.

(3) ***"Confidential"*** shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security that the Original Classification Authority is able to identify or describe.

(c) ***Classified National Security Information*** is any data, file, paper, record, or computer disc containing information associated with the national defense or foreign relations of the United States that requires protection against unauthorized disclosure and is marked (Top Secret, Secret, or Confidential) to indicate its classified status when in documentary form.

(d) ***Derivative Classification*** is the incorporation, paraphrasing, restating or generating in new form information that is already classified, and marking the newly developed material consistent with the Classification markings that apply to the source information.

Derivative Classification includes the Classification of information based on Classification guidance.

(e) ***Infraction and Violation Program*** is the disciplinary and security clearance program that addresses Security Infractions and Security Violations by Peace Corps employees and contractors.

(f) ***Need-to-know*** is the necessity for Access to, or knowledge or possession of, specific information required to carry out official duties.

(g) ***Original Classification Authority*** is authority granted by the President or by an official delegated that authority from the President to make an initial determination that new or previously unclassified information is classified. No one in the Peace Corps has this authority.

(h) ***Security Incident*** is an event that results in the failure to safeguard classified materials in accordance with Executive Order 13526, "Classified National Security Information", Department of State Foreign Affairs Manual (FAM) 12 FAM 500, and this chapter. The consequence of a Security Incident is either a Security Infraction or a Security Violation.

(i) ***Security Information Program*** is the program for the safety and security of Classified National Security Information established under Executive Order 13526.

(j) ***Security Infraction*** is a failure to properly safeguard classified material that does not result in the actual or probable compromise of the material e.g., improperly stored classified material within a controlled Access area.

(k) ***Security Violation*** is a failure to properly safeguard confidential or secret classified material that results in the actual or probable compromise of the material, or any Security Incident involving the mishandling of Top Secret, Special Access Program, and Sensitive Compartmented Information, regardless of location or probability of compromise.

6.0 Responsibilities

6.1 Peace Corps Director

The Director of the Peace Corps has the responsibility to:

(a) demonstrate personal commitment and commit senior management to the successful implementation of the program established under Executive Order 13526;

(b) commit necessary resources to the effective implementation of the program established under Executive Order 13526; and

(c) designate a senior agency official to direct and administer the program.

6.2 Associate Director for Safety and Security

The Associate Director for Safety and Security is the designated senior agency official responsible for the direction and administration of the Peace Corps Security Information Program established under Executive Order 13526 and, in performing this function, must:

(a) manage the establishment and oversight of such program in accordance with Executive Order 13526;

(b) promulgate implementing procedures for the program; and

(c) establish and maintain an ongoing self-inspection program, which must include the periodic review and assessment of the Peace Corps classified information.

6.3 Chief, Information and Personnel Security Division

The Chief of the Information and Personnel Security Division (IPS), who reports to the Associate Director for Safety and Security, has day-to-day responsibility for the Peace Corps Security Information Program and must:

(a) develop and implement the agency's information security program in accordance with Federal directives and this Manual Section to prevent unauthorized Access through the control of the Access to and handling, storage and destruction of classified information;

(b) develop contingency plans for the safeguarding of classified information;

(c) develop and manage the Infraction and Violation Program for the agency;

(d) report on activities associated with the information security program as required by the Information Security Oversight Office of the National Archives and Records Administration; and

(e) establish and maintain a security education and training program.

6.4 Chief, Emergency Management and Physical Security Division

The Chief of the Emergency Management and Physical Security Division (EMPS), who reports to the Associate Director for Safety and Security, must ensure that all required physical security safeguards are in place for the storage and destruction of Classified National Security Information, in accordance with established Federal standards.

6.5 Employees

Employees with access to Classified National Security Information must comply with the established procedures for safeguarding Classified National Security Information and report observed deficiencies or suspected Security Incidents to the Chief of IPS.

7.0 Requirements for Access to Classified National Security Information

7.1 Determination of Need for Access

The Chief of IPS must conduct sensitivity surveys of all positions within the Peace Corps to determine the need for access to Classified National Security Information and the level of investigation required prior to granting Access.

7.2 Access to Classified National Security Information

Employees and contractors of Peace Corps can only be given access to Classified National Security Information when they have been granted a security clearance by the Peace Corps commensurate with the level of information to which they require Access and have received a Classified National Security Information briefing.

7.2.1 Refresher Briefings/Training

All employees and contractors who hold security clearances must attend a refresher briefing or complete refresher training at least once a year.

7.2.2 Termination Briefings

All employees and contractors given access to Classified National Security Information must receive a termination briefing when they terminate their service with the Peace Corps.

Any employee or contractor given access to Classified National Security Information whose clearance is withdrawn must be given a termination briefing.

7.2.3 Mandatory Performance Rating Element

The annual performance plan of all personnel whose duties involve the handling of classified information must contain a critical element regarding their performance of duties relating to the management of classified information. Deliberate or excessive Security Infractions or Security Violations represent performance inconsistent with the expectations and criteria for awarding a performance bonus or promotion.

8.0 Control of Classified National Security Information in Peace Corps Facilities

Classified National Security Information processing (reading, storage, destruction, and discussion) will normally occur only at the Peace Corps Headquarters and will be restricted to the secret or confidential level. Classified information may be processed only at a Regional Recruiting Office in conjunction with a continuity of operations event.

Classified National Security Information may not be brought into any Peace Corps facility overseas. Any discussion or reading of Classified National Security Information overseas must only occur in an approved area within a U.S. embassy or consulate.

8.1 Annual Reviews and Inspections

IPS must conduct annual reviews of all domestic Peace Corps offices that hold classified information to insure compliance with established policies and procedures.

9.0 Original Classification Authority

Peace Corps does not have Original Classification Authority. Therefore, employees or contractors may not create and classify material.

10.0 Derivative Classification

Peace Corps staff who will be making Derivative Classification actions shall receive training in the proper application of the Derivative Classification principles. Derivative classifiers who do not receive such training at least once every 2 years shall have their authority to apply Derivative Classification markings suspended until they have received such training. A waiver may be granted by the agency head, the deputy agency head, or the senior agency official if an individual is unable to receive such training due to unavoidable circumstances. Whenever a waiver is granted, the individual shall receive such training as soon as practicable.

11.0 Classification Challenges

Authorized holders of information, which are those granted Access as defined in section 5.0(a), who, in good faith, believe that its Classification status is improper are encouraged and expected to challenge the Classification status of the information. The challenge should initially be informal. A request should be made in writing to the original classifier to review the Classification level.

12.0 Security Infraction and Violation Program

An employee or contractor who commits Security Infractions or Security Violations, or a supervisor who fails to insure effective organizational security procedures, may be subject to administrative, disciplinary, or security clearance actions initiated, as appropriate, by the Office of Human Resources Management, the Office of Acquisitions and Contract Management or IPS.

Disciplinary and security clearance actions will be handled on a case by case basis and will be influenced by the severity of the incident and the security history of the offender.

To facilitate the management of the Infraction and Violation Program, the Chief of IPS will maintain files on any employee who has incurred a Security Infraction or Security Violation and will provide written notification to the employee's supervisor so that the infraction can be taken into account during the annual performance review.

13.0 Reporting to Information and Security Oversight Office

The Chief of IPS is responsible for the compilation of all reports to the Information and Security Oversight Office of the National Archives and Records Administration.

14.0 Effective Date

The effective date is the date of issuance.