



Environmental Management Consolidated Business Center (EMCBC)

Subject: EMCBC Site Operations Security (OPSEC) Program Plan

PROGRAM PLAN

APPROVED: Signature on File
EMCBC Assistant Director of
Technical Support & Asset Management

1.0 PURPOSE

This document identifies the requirements and makeup of the Environmental Management Consolidated Business Center (EMCBC) Operations Security (OPSEC) Program Plan, provides direction of the program, assigns responsibility and implements National Security Decision Directive 298, and DOE Order 471.6.

2.0 SCOPE

This Program Plan applies to all EMCBC personnel, including contractors directly supporting the EMCBC.

3.0 APPLICABILITY

This Program Plan applies to all EMCBC employees working at the EMCBC Chiquita Center facility and EMCBC employees who physically work at an alternate location, but are supervised by an EMCBC employee and serviced by EMCBC's Office of Human Resources (OHR). This Program Plan also applies to the employees at EMCBC Service Level Agreement sites that choose to adopt it.

4.0 REQUIREMENTS

- 4.1 National Security Decision Directive (NSDD) 298, "National Operations Security Program," January 22, 1988.
- 4.2 DOE Order 471.6, "Information Security, Admin Change 1," November 23, 2012.

5.0 DEFINITIONS

Countermeasure - Anything that effectively negates or reduces the risk from an adversary's ability to exploit vulnerabilities.

Critical Information - Information that must be protected from loss to keep an adversary from gaining a significant operational, economic, political, or technological advantage.

Indicators - Any detectable activity or other information that, either by itself or when aggregated, gives an adversary insight into critical or sensitive information.

OPSEC - A systematic and analytic process to deny potential adversaries information about capabilities and intentions by identifying, controlling, and protecting evidence of the planning and execution of sensitive activities and operations.

OPSEC Assessment - An assessment of the effectiveness of the OPSEC Program, and any associated security or counterintelligence programs deemed appropriate by the requesting Under Secretary, Director, or manager. An OPSEC Assessment generally involves a team of OPSEC analysts and other security experts, and assesses the OPSEC program in regards to a specific activity or operation. The OPSEC Assessment Team uses the OPSEC process to give the requesting authority a report on risks associated with identified vulnerabilities, and recommended countermeasures.

OPSEC Manager - The individual designated by Headquarters, a field element, or a DOE contractor to be responsible for and provide direction to the DOE OPSEC program within their specific area of responsibility.

OPSEC Program Manager - The individual designated by the Director, Office of Safeguards and Security, to be the primary point of contact for the OPSEC Program and to serve as an interface for DOE with the national OPSEC community. The OPSEC Program Manager is responsible for and provides direction to the DOE OPSEC Program.

OPSEC Working Group - A formally designated body representing a broad range of administrative and programmatic activities at Headquarters, field elements, or contractor facilities which provides review, support, and participation with senior management in the implementation and furtherance of their OPSEC Program.

Risk Assessment - The process of evaluating security risks based on analysis of threats to and vulnerabilities of a system or operation.

Security Threat - The technical and operational capability of an adversary to detect and to exploit vulnerabilities.

Threat Analysis - An examination of an adversary's technical and operational capabilities, motivation, and intentions to detect and exploit security vulnerabilities.

Vulnerability - The susceptibility of critical information to the exploitation of the adversary.

6.0 BACKGROUND

6.1 National Security Decision Directive 298 was signed by President Reagan in January 1988 and calls for each Executive Department and agency substantially

involved in supporting national security missions with classified or sensitive activities to establish a formal OPSEC Program.

- 6.2 Security programs and procedures already exist to protect classified matter. However, information generally available to the public as well as certain detectable activities reveal the existence of, and sometimes detail about, classified or sensitive undertakings. Such indicators may assist those seeking to neutralize or exploit U.S. Government actions in the area of national security. Application of the OPSEC process promotes operational effectiveness by helping prevent the inadvertent compromise of sensitive or classified U.S. Government activities, capabilities, or intentions.
- 6.3 The OPSEC process involves five steps: identification of critical information, analysis of threats, analysis of vulnerabilities, assessment of risks, and application of appropriate countermeasures. The process begins with an examination of the totality of an activity to determine what exploitable but unclassified evidence of classified activity could be acquired in light of known collection capabilities of potential adversaries. Such evidence usually derives from openly available data. Certain indicators may be pieced together or interpreted to discern critical information. Indicators most often stem from routine administrative, physical, or technical actions taken to prepare for or execute a plan or activity. Once identified, they are analyzed against the threat to determine the extent to which they may reveal critical information. Managers then use these threat and vulnerability analyses in risk assessments to assist in the selection and adoption of countermeasures.

7.0 RESPONSIBILITIES

- 7.1 The EMCBC Director will appoint in writing the EMCBC OPSEC Manager and each member of the OPSEC Working Group. Additionally, the Director will provide support to the OPSEC program, as necessary.
- 7.2 The EMCBC OPSEC Manager shall:
 - 7.2.1 Implement OPSEC in accordance with DOE policies, procedures, and planning guidance, as necessary.
 - 7.2.2 Conduct an annual review of OPSEC practices to assist in the improvement of OPSEC program.
 - 7.2.3 Establish and chair EMCBC OPSEC working group to provide a forum to discuss generic and specific OPSEC issues. As a minimum the working group will consist of representatives from the following Offices: Director, Contracting, Cost Estimating and Project Management Support, Financial Management, Human Resources, Information Resource Management, Chief Counsel, EMCBC

Classification Office (Building 55), and Technical Support and Asset Management. Other offices and functions may be invited to attend, or may request to participate in the working group.

7.2.4 Support OPSEC programs and efforts by other government departments and agencies, as requested.

7.2.5 Delegate authority to plan, direct and implement OPSEC measures, as appropriate, to the EMCBC OPSEC Working Group.

7.2.6 Ensure all staff elements receive appropriate training and/or OPSEC awareness information according to the following requirements:

7.2.6.1 Senior staff will receive an executive OPSEC overview from the EMCBC OPSEC Manager.

7.2.6.2 OPSEC Working Group members will complete the OPSEC Fundamentals Computer Based Training.

7.2.6.3 All EMCBC personnel will receive initial OPSEC awareness training. Awareness training may be included in the EMCBC Initial Security Awareness Briefing.

7.3 EMCBC OPSEC Working Group shall:

7.3.1 Establish an OPSEC Program in accordance with the provisions of both the NSDD 298 and DOE O 471.6. This shall include identifying Critical Information.

7.3.2 Carry out specific OPSEC requirements as directed by the EMCBC OPSEC Manager.

7.3.3 Conduct an annual review and evaluation of the OPSEC Program to determine its effectiveness in the preceding year and to develop recommendations on improvements for the next year and the longer term.

7.3.4 Determine requirements for OPSEC measures by contractors. Ensure that these requirements are made known to the EMCBC Contracting Officer who will notify the contractor as soon as possible and ensure the requirements are incorporated specifically into Requests For Proposals and subsequent contractual documents in sufficient detail to enable cost estimates and compliance with OPSEC measures by contractors.

7.3.5 Recommend to the EMCBC OPSEC Manager changes to policies, procedures, or practices to the EMCBC OPSEC Program.

7.3.6 Issue OPSEC planning guidance for activities within their area of responsibility.

8.0 GENERAL INFORMATION

- 8.1 In accordance with NSDD 298 and DOE Order 471.6, the EMCBC will implement a viable and effective OPSEC Program.
- 8.2 In accordance with NSDD 298, the EMCBC will address OPSEC from the beginning of all planning, programming and budgeting actions and will address OPSEC during all operations and activities.
- 8.3 A necessary condition for maintaining essential secrecy is protection of classified and unclassified critical information ensuring that besides the application of traditional security measures, the EMCBC maintains a heightened awareness of potential threats of adversaries taking advantage of publicly available information and other detectable unclassified activities to derive indicators of U.S. intentions, capabilities, operations, and activities.
- 8.4 In accordance with DOE Order 471.6, the EMCBC must identify and document its Critical Information (CI).
- 8.5 Review and update its CI documentation as necessary to reflect current assets, threats, operations and other relevant factors.
- 8.6 Provide the information required for sound risk-management decisions concerning the protection of sensitive information to the decision makers who are responsible for mission accomplishment.
- 8.7 Ensure CI is not included on publically available website by encouraging or requiring reviews of information being proposed for placement on such websites.

EMCBC RECORD OF REVISION

DOCUMENT - EMCBC Site Operations Security (OPSEC) Program Plan

If there are changes to the controlled document, the revision number increases by one. Indicate changes by one of the following:

- I Placing a vertical black line in the margin adjacent to sentence or paragraph that was revised.
- I Placing the words GENERAL REVISION at the beginning of the text.

Rev. No.	Description of Changes	Revision on Pages	Date
0	NA, 1 st Edition to meet requirement	NA	05/07/13