OPSEC PROGRAM POLICY TEMPLATE

[ORGANIZATION] OPSEC Program Policy
[DATE]

Subject: [ORGANIZATION] OPERATIONS SECURITY PROGRAM

1. PURPOSE. This Order establishes the [ORGANIZATION] Operations Security (OPSEC) Program, provides policy, assigns responsibility and implements [Add Policy Reference]

2. SCOPE.
    a. This Order applies to all [ORGANIZATION] and all personnel assigned.
    b. All organizations and agencies subordinate to the [ORGANIZATION].
    c. All contractors providing support to [ORGANIZATION] activities and operations.

3. REFERENCES.
    a. Add references.

4. DEFINITIONS.
    a. **OPSEC**. A security discipline designed to deny adversaries the ability to collect, analyze, and exploit information that might provide an advantage against the United States by preventing inadvertent compromise of Critical Information through a process of continual assessment that identifies and analyzes Critical Information, vulnerabilities, risks, and external threats.
    b. **OPSEC Coordinators.** Staff members assigned responsibilities to implement the [ORGANIZATION] OPSEC Program within their functional area or the organization.
    c. **Critical Information.** Information that must be protected from loss to keep an adversary from gaining a significant operational, economic, political, or technological advantage.
    d. **Indicators.** Any detectable activity or other information that, either by itself or when aggregated, gives an adversary insight into critical or sensitive information.
    e. **Risk Assessment**. The process of evaluating security risks based on analysis of threats to and vulnerabilities of a system or operation.
    f. **Threat Analysis.** An examination of an adversary's technical and operational capabilities, motivation, and intentions to detect and exploit security vulnerabilities.
    g. **Countermeasure**. Anything that effectively negates or reduces the risk from an adversary's ability to exploit vulnerabilities.
    h. **adversary**. An individual, group, organization, or government that must be denied critical information.
    i. **Vulnerability.** The susceptibility of critical information to the exploitation of the adversary.
    j. **OPSEC Assessment**. An assessment of the effectiveness of the OPSEC Program, and any associated security or counterintelligence programs deemed appropriate by the requester. 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

k. **OPSEC Assessment Team** uses the OPSEC cycle to give the requesting authority a report on risks associated with identified vulnerabilities, and recommended countermeasures.

5. BACKGROUND.
   a. Statement regarding policy.
   b. Security programs and procedures already exist to protect classified matters. 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 cycle promotes operational effectiveness by helping prevent the inadvertent compromise of sensitive or classified U.S. Government activities, capabilities, or intentions.
   c. The OPSEC cycle involves identification of critical information, analysis of threats, analysis of vulnerabilities, assessment of risks, and application of appropriate countermeasures continuously repeated to assess effectiveness. The cycle 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.

6. POLICY.
   a. In accordance with [POLICY], [ORGANIZATION] will implement a viable and effective OPSEC Program. [ORGANIZATION] will also cooperate with other departments, agencies, and institutions to minimize damage to national security when OPSEC issues arise.
   b. A necessary condition for protecting critical information and indicators is ensuring that besides the application of traditional security measures, the [ORGANIZATION] 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.
   c. Extraordinary protection of [ORGANIZATION] acquisition programs, activities, or operations and their attendant costs for protecting critical information and indicators through the OPSEC cycle are balanced against the potential loss to mission effectiveness.

7. RESPONSIBILITIES.

a. The [POC], has responsibility for policies and procedures relating to the [ORGANIZATION] OPSEC Program. The [POC] Director will provide [ORGANIZATION]-wide guidance and assistance in OPSEC matters.
b. The [POC] is the [ORGANIZATION] OPSEC Program Manager. As the [ORGANIZATION] OPSEC Program Manager, he/she shall:
    i. Develop OPSEC policies, procedures, and planning guidance.
    ii. Conduct an annual review of OPSEC procedures to assist in the improvement of OPSEC programs.
    iii. Receive annual OPSEC reports from [ORGANIZATION] Directorates, Offices, and Functions, and prepare an overarching annual report.
    iv. Establish and chair a/an [ORGANIZATION] OPSEC working group to provide a forum to discuss generic and specific OPSEC issues. At a minimum, the working group will consist of representatives from [ELEMENTS THAT WILL PARTICIPATE IN THE WORKING GROUP]. Other Offices and Functions may be invited to attend, or may request to participate in the working group.
    v. Coordinate OPSEC matters concerning more than one Directorate or Office, as requested.
    vi. Coordinate mutual support between Directorates and other departments and agencies, as requested.
    vii. Provide OPSEC planning, support, and advice for [ORGANIZATION] Headquarters senior officials and staff elements.
    viii. Support OPSEC programs and efforts by other government departments and agencies, as requested.
    ix. Delegate authority to plan, direct and implement OPSEC measures, as appropriate, to [POC].
    x. Ensure all staff elements receive appropriate training and/or OPSEC awareness information according to the following requirements:
        1. Senior staff will receive an executive OPSEC overview from [POC].
        2. OPSEC Coordinators and OPSEC Working Group members will complete either the OPSEC Fundamentals CBT or a minimum of a four-hour OPSEC Fundamentals course; the [ORGANIZATION] OPSEC Working Group may direct additional training requirements based on current situation or other significant threat changes.
        3. OPSEC Analysts will complete an OPSEC Practitioners' Course.
        4. All personnel will receive initial awareness training within [##] days of assignment to [ORGANIZATION], or within [##] days of beginning a position as a new hire.
        5. All personnel will receive awareness training a minimum of [# HOURS] annually, or more often according to direction of the [POC].
c. The [POC] is responsible for the provision of OPSEC support to all [ORGANIZATION] staff elements and [ORGANIZATION] partners. As such, he/she shall:

i. Provide consultation on the development of OPSEC programs and plans, and the conduct of OPSEC surveys.
ii. Provide a curriculum of formal OPSEC courses including, as a minimum, an OPSEC Fundamentals course and an OPSEC Practitioner's Course.
iii. The OPSEC Fundamentals course will provide the workforce with an understanding of the OPSEC cycle.
iv. The OPSEC Practitioner's Course will provide the student with all skills and tools necessary to apply the OPSEC cycle to planning and operations, to obtain accurate and timely threat information, to assess OPSEC vulnerabilities and risks, and to develop effective countermeasures. The Practitioner's Course will address fundamentals of OPSEC program development, management and planning.
v. The Senior Executive OPSEC Overview will provide an understanding of the OPSEC cycle, how OPSEC can contribute to mission effectiveness, and the process to engage [ORGANIZATION] OPSEC professionals as required.
vi. Provide assistance with the development of OPSEC training materials as requested by specified customers.
vii. Provide awareness materials for all specified customers.
viii. Provide OPSEC marketing materials for all specified customers.

d. Headquarters Staff Elements shall:
i. Establish an OPSEC Program in accordance with the provisions of Paragraph 6.a, above.
ii. Identify an employee in their area of responsibility to serve as an OPSEC Coordinator. The OPSEC Coordinator will perform OPSEC related actions and be a focal point for OPSEC matters.
iii. Plan and implement specific OPSEC requirements as directed by the [ORGANIZATION] OPSEC Officer.
iv. Establish measures to ensure that all personnel, commensurate with their positions and security clearances, are aware of hostile intelligence threats and understand the OPSEC cycle.
v. Establish requirements for an annual review and evaluation of OPSEC procedures to assist in the improvement of the OPSEC Program. 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. Submit a report of these annual reviews to the [ORGANIZATION] OPSEC Program Manager. Establish provisions for inter and intra-agency support and cooperation with respect to OPSEC programs.
vi. Provide management, review, and inspection of their OPSEC Programs.
vii. Determine requirements for OPSEC measures by contractors. Ensure that these requirements provided to the contractor as soon as possible and 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.

viii. Recommend to the [ORGANIZATION] OPSEC Program Manager changes to policies, procedures, or practices to the [ORGANIZATION] OPSEC Program.
ix. Develop OPSEC concepts and establish policies and procedures to supplement those developed by the [ORGANIZATION] OPSEC Program Manager.
x. Issue OPSEC planning guidance for activities within their area of responsibility.
xi. Ensure adequate capabilities to execute OPSEC measures.
xii. Inform the [ORGANIZATION] OPSEC Program Manager of OPSEC assessments that they conduct with other government departments and agencies. This should be done at the time of the OPSEC assessment.
xiii. In addition to the responsibilities listed for Staff Elements, the organizations listed below will ensure the creation and management of OPSEC programs which encourage and ensure the integration of OPSEC into operations of all subordinate elements of their organization. Other offices and functions may be required to do the same based upon recommendation of the OPSEC Working Group. These organizations are: [LIST]

8. IMPLEMENTATION. Where appropriate, organizations and sub organizations, and other staff elements should develop additional guidance required to implement this Order and provide a copy of that guidance to the [ORGANIZATION] OPSEC Program Manager within six months of this guidance.