SYSTEM II
90944

THE WHITE HOUSE

WASHINGTON

January 22, 1988

NATIONAL SECURITY DECISION
DIRECTIVE NUMBER 298

NATIONAL OPERATIONS SECURITY PROGRAM

OBJECTIVE

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 details about, classified or sensitive information or undertakings. Such indicators may assist those seeking to neutralize or exploit U.S. Government actions in the area of national security. Application of the operations security (OPSEC) process promotes operational effectiveness by helping prevent the inadvertent compromise of sensitive or classified U.S. Government activities, capabilities, or intentions.

OPSEC PROCESS

The operations security 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 the 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 the 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. Commanders and managers then use these threat and vulnerability analyses in risk assessments to assist in the selection and adoption of countermeasures.

OPSEC thus is a systematic and proved process by which the U.S. Government and its supporting contractors can deny to potential adversaries information about capabilities and intentions by identifying, controlling, and protecting generally unclassified evidence of the planning and execution of sensitive Government activities.

APPLICATION

Indicators and vulnerabilities are best identified through detailed OPSEC planning before activities start. They may also be identified during or after the conduct of routine functional activities by analyzing how functions are actually performed and the procedures used. Planning and analysis proceed from the adversary's perspective. To assist in OPSEC planning and analysis, OPSEC planning guidance must be developed jointly by those most familiar with the operational aspects of a particular activity together with their supporting intelligence elements.

OPSEC planning guidance should take account of those aspects of an activity that should be protected in light of U.S. and adversary goals, estimated key adversary questions, probable adversary knowledge, desirable and harmful adversary appreciations, and pertinent intelligence threats. OPSEC planning guidance should also outline OPSEC measures to complement physical, information, personnel, signals, computer, communications, and electronic security measures. OPSEC measures may include, but are not limited to, counterimagery, cover, concealment, and deception.

In the OPSEC process, it is important to distinguish between analysis of threat and vulnerability, on the one hand, and implementation, on the other. Recommendations on the use of OPSEC measures are based on joint operational-intelligence analyses, but ultimate decisions on implementation are made by commanders, supervisors, or program managers who determine the aspects of a program or activity to be protected. The decision-maker with ultimate responsibility for mission accomplishment and resource management must have complete authority for determining where and how OPSEC will be applied.

POLICY

A National Operations Security Program is hereby established. Each Executive department and agency assigned or supporting national security missions with classified or sensitive activities shall establish a formal OPSEC program with the following common features:

-- Specific assignment of responsibility for OPSEC direction and implementation.

-- Specific requirements to plan for and implement OPSEC in anticipation of and, where appropriate, during department or agency activity.

-- Direction to use OPSEC analytical techniques to assist in identifying vulnerabilities and to select appropriate OPSEC measures.

-- Enactment of measures to ensure that all personnel, commensurate with their positions and security clearances, are aware of hostile intelligence threats and understand the OPSEC process.

-- Annual review and evaluation of OPSEC procedures so as to assist the improvement of OPSEC programs.

-- Provision for interagency support and cooperation with respect to OPSEC programs.

Agencies with minimal activities that could affect national security need not establish a formal OPSEC program; however, they must cooperate with other departments and agencies to minimize damage to national security when OPSEC problems arise.

ACTION

Heads of Executive departments and agencies assigned or supporting national security missions.

Heads of Executive departments or agencies with national security missions shall:

-- Establish organizational OPSEC programs;

-- Issue, as appropriate, OPSEC policies, procedures, and planning guidance; and

-- Designate departmental and agency planners for OPSEC.

Further, they shall advise the National Security Council (NSC) on OPSEC measures required of other Executive departments and agencies in order to achieve and maintain effective operations or activities. In this connection, the Joint Chiefs of Staff shall advise the NSC of the impact of nonmilitary U.S. policies on the effectiveness of OPSEC measures taken by the Armed Forces, and recommend to the NSC policies to minimize any adverse effects.

Chairman, Senior Interagency Group for Intelligence (SIG-I).

Consistent with previous Directives, the SIG-I has responsibility for national OPSEC policy formulation, resolution of interagency differences, guidance on national-level OPSEC training, technical OPSEC support, and advice to individual Executive departments and agencies. The National Operations Security Advisory Committee (NOAC), as part of the SIG-I structure and functioning under the aegis of the Interagency Group for Countermeasures (Policy), will:

-- Advise the SIG-I structure on measures for reducing OPSEC vulnerabilities and propose corrective measures;

-- As requested, consult with, and provide advice and recommendations to, the various departments and agencies concerning OPSEC vulnerabilities and corrective measures;

-- On an ad hoc basis, chair meetings of representatives of two or more Executive departments or agencies having competing interests or responsibilities with OPSEC implications that may affect national security interests. Analyze the issues and prepare advisory memoranda and recommendations for the competing agencies. In the event NOAC fails to resolve differences, it shall submit the issue, together with its recommendation, to the SIG-I for resolution, which may recommend a meeting of the Policy Review Group (PRG) to consider the issue;

-- Bring to the attention of the SIG-I unsolved OPSEC vulnerabilities and deficiencies that may arise within designated programs and activities of the Executive branch; and

-- Specify national-level requirements for intelligence and counterintelligence OPSEC support to the SIG-I.

Director, National Security Agency.

The Director, National Security Agency, is designated Executive Agent for interagency OPSEC training. In this capacity, he has responsibility to assist Executive departments and agencies, as needed, to establish OPSEC programs; develop and provide interagency OPSEC training courses; and establish and maintain an Interagency OPSEC Support Staff (IOSS), whose membership shall include, at a minimum, a representative of the Department of Defense, the Department of Energy, the Central Intelligence Agency, the Federal Bureau of Investigation, and the General Services Administration. The IOSS will:

-- Carry out interagency, national-level, OPSEC training for executives, program and project managers, and OPSEC specialists;

-- Act as consultant to Executive departments and agencies in connection with the establishment of OPSEC programs and OPSEC surveys and analyses; and

-- Provide an OPSEC technical staff for the SIG-I.

Nothing in this directive:

-- Is intended to infringe on the authorities and responsibilities of the Director of Central Intelligence to protect intelligence sources and methods, nor those of any member of the Intelligence Community as specified in Executive Order No. 12333; or

-- Implies an authority on the part of the SIG-I Interagency Group for Countermeasures (Policy) or the NOAC to examine the facilities or operations of any Executive department or agency without the approval of the head of such Executive department or agency.