Approved for release by NSA on 12-01-2011, Transparency Case# 63852

The National OPSEC Program

STATUTORILY EXEMPT

This article is a reprint of the monograph published by the Interagency OPSEC Support Staff in April 1990. It provides some background on Operations Security (OPSEC) and a discussion of the provisions of the National Security Decision Directive (NSDD) establishing the National OPSEC Program. The paper also contains a description of the organization and activities of the Interagency OPSEC Support Staff (IOSS).

In today's information age, the effective conduct of government activities requires increased efforts to ensure that our adversaries do not obtain data that would allow them to achieve their objectives or undermine ours. Concerns over the inadvertent compromise of sensitive or classified U.S. government activities, capabilities, and intentions led the president to approve a National Security Decision Directive establishing a National Operations Security Program. The NSDD sets up a national operations security structure and requires each executive department and agency assigned or supporting national security missions with classified or sensitive activities to establish an OPSEC program.

The NSDD describes OPSEC as "... 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."

This monograph attempts to present an overview of the origins of OPSEC, how it works, what the NSDD requires, and why OPSEC is important enough to be the subject of a presidential directive.

There Is Nothing New about OPSEC

There is nothing new about the principles underlying OPSEC. If you have given a surprise birthday party or attempted to make your house look lived in while you were on vacation by arranging for someone to pick up your newspapers and installing a light timer, you have practiced OPSEC. OPSEC is applicable to any situation where you want to deny information to an outsider in order to achieve your mission goals. What is relatively new is the development of a methodology whereby the principles behind OPSEC can be applied in a consistent and thorough manner.

OPSEC as a methodology originated during the Vietnam conflict when a small group of individuals was assigned the mission of finding out how the enemy had been obtaining advance information of certain combat operations in Southeast Asia. This team was established by the Commander in Chief, Pacific, and given the cover name PURPLE DRAGON. Their initial mission was to review several air operations. It soon became apparent to the team that although traditional security and intelligence countermeasures programs were in place in Southeast Asia, reliance solely upon them was insufficient to deny critical information to the enemy, especially information relating to intentions and capabilities. A new approach was needed to deal with unclassified information and indicators that could be pieced together by enemy intelligence to derive critical information. The group conceived and developed the methodology of analyzing U.S. operations from the enemy viewpoint to find out how the enemy obtained the information. They determined what information needed protection, obtained information on the enemy's intelligence capabilities, uncovered the vulnerabilities of the U.S. operations to enemy exploitation, assessed the risk of exploitation, and devised ways to thwart the enemy's collection or use of the data. They then recommended corrective actions to the local commanders for adoption. They were successful in what they did, and, to name what they had done, they coined the term "operations security."

This OPSEC methodology has now been around for more than twenty years. Over the years it became increasingly apparent that OPSEC had utility in virtually every government program that had information needing protection to assure program effectiveness. Techniques have been modified and improved by OPSEC practitioners as experience has been gained with many different organizations and in areas far afield from military combat operations. Today it is understood that OPSEC is as applicable to an administrative or research and development activity as it is to a combat operation.

How OPSEC Works

One of the most important lessons learned over the last two decades of OPSEC experience is that most government activities involve a stereotyped sequence or pattern of events, some planned and some unplanned, unique to that organization or activity. Those events and their components, which occur during the planning, preparatory, and execution stages of an activity, create vulnerabilities that even in the securest of environments may be subject to adversary exploitation. Through the analysis of actions and data relating to these stages, it can be determined how adversaries can obtain an organization's critical information even if completely denied access to all classified and sensitive aspects of the activity by effective security measures and intelligence countermeasures.

The detectable activities and bits of data that can be pieced together to derive classified or sensitive information are called indicators. Typically the individual indicators are considered unclassified and are often beyond the purview of traditional security programs to even identify, let alone classify and protect. Indicators may occur

throughout a broad spectrum of activities, undertaken both by the organization involved and by supporting organizations. Usually, indicators most easily accessible to the adversary occur in support activities like administration, budgeting, communications, databases, logistics, maintenance, etc.

In the past, many indicators were naturally protected by distance and time. Information processing, storage and transmission have evolved, over the years, to a point that most information is very susceptible to adversary acquisition. In addition, even the most unsophisticated adversaries have at their disposal collection devices and techniques that reflect the technological age in which we live – a technology that can be used to overcome many of the protective techniques conceived in a much simpler world.

Today, if OPSEC is not integrated into sensitive and classified government activities, chances are very great that our adversaries will acquire significant information about the activities. It probably would have been difficult for the PURPLE DRAGON team to foresee that twenty years later the methodology they had developed would become a national program. However, in retrospect, it seems inevitable that such an evolution should have occurred.

The Five-Step OPSEC Process

The NSDD formalized OPSEC and described it as a five-step process: identification of critical information, analysis of threats, analysis of vulnerabilities, assessment of risks, and application of countermeasures.

The following paragraphs discuss the elements and application of the OPSEC process. Although the NSDD describes the process as discrete steps, they are most often applied in parallel with some elements repeated several times. The process must be tailored to the specific organization and activity being analyzed. Most importantly, the process is a cycle where after countermeasures are implemented, evaluation must continue.

Basic to the process is determining what information, if available to one or more adversaries, would harm an organization's ability to effectively carry out the operation or activity. This critical information constitutes "core secrets" of the organization, i.e., the few nuggets of information that are central to the organization's mission or the specific activity. Critical information usually is, or should be, classified or at least protected as sensitive unclassified information. Sometimes the information that is critical and must be protected is another organization's core secrets, this being especially true in support functions.

Knowing who the adversaries are and what information they require to meet their objectives is essential in determining what information is truly critical to an organization's mission effectiveness. In any given situation there is likely to be more than one adversary, and each may be interested in different types of information. For example, a terrorist may want information about a dignitary's movements, while a hostile country's intelligence service may want to know what that person is working on.

The adversary's ability to collect, process, analyze, and use information, i.e., the threat, must also be determined. The objective is to know as much as possible about each adversary and the strategies available for targeting the organization. It is especially important to tailor the adversary threat to the actual activity and, to the extent possible, determine what the adversary's capabilities are for the specific time and place of the activity.

Determining the organization's vulnerabilities involves systems analyses of how the operation or activity is actually conducted by the primary and supporting organizations. The organization and the activity must be reviewed as the adversaries will view it, thereby providing the basis for understanding how the organization really operates and what are the true, rather than hypothetical, vulnerabilities. The chronology of all events, the timing of actions, and the flow of information and materials must be reviewed. Actions that can be observed or data that can interpreted or pieced together to derive critical information must be identified. An assessment should be made of the vulnerability to the adversary actually collecting the data that can provide the critical information.

Vulnerabilities and specific threats must be matched. Where the vulnerabilities are great and the adversary threat is evident, adversary exploitation is expected. Therefore, a high priority for protection needs to be assigned and corrective action taken. Where the vulnerability is slight and the adversary has a marginal collection capability, the priority should be low.

Countermeasures that will do away with the vulnerabilities, threats or utility of the information to the adversaries should be developed. The possible countermeasures should include alternatives that may vary in both effectiveness, feasibility, and cost. Countermeasures may include procedural changes, deception and perception management, intelligence countermeasures, traditional security measures, or anything that is likely to work in the particular situation.

The impact of the loss of the critical information on the effectiveness of the activity is balanced against the cost of implementing corrective measures. The probability that the information will be collected and used by the adversary is then factored in. The manager can then implement those countermeasures that are deemed appropriate and cost effective. The authority for determining where and how countermeasures will be applied must rest with the decision maker who has ultimate responsibility for mission accomplishment and resource management.

In some cases, there may be no way to protect the information because of cost or other factors, making implementation impossible. When this occurs, the manager must decide to either accept the degradation to effectiveness or cancel the operation.

The OPSEC process should be carried out by operations elements of an organization or component with the advice and assistance of OPSEC and other technical experts as required. OPSEC must be integrated into the activity from conception and initiation of planning and extend throughout the life of the activity.

By using the OPSEC process, managers will have a better understanding of how their organization actually operates, what information may be available to adversaries, the impact of the loss of the information on mission effectiveness, and ways to protect that information. Most significant, the decision of whether to implement countermeasures must be based on the manager's cost benefit analysis and an evaluation of the overall program objectives.

OPSEC is a systematic process that can be applied by organizations to deny to potential adversaries information about capabilities and intentions by identifying, controlling, and protecting generally unclassified information and evidence of the planning and execution of sensitive and classified activities.

OPSEC Program Requirements

The NSDD requires formal OPSEC programs for each executive department and agency assigned or supporting national security missions. It also describes the OPSEC process and provides guidance on the application of the OPSEC process within departments' and agencies' activities. The NSDD recognizes that not all agencies are directly involved in classified or sensitive activities. It exempts those agencies with only minimal activities that could affect national security from establishing a formal program.

The responsibility for the development, implementation, and maintenance of a department's or agency's OPSEC program rests with the head of the department or agency. The NSDD allows a great deal of latitude on how the program should be implemented, but it does require that all programs have, as a minimum, the following 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 analytic techniques to assist in identifying vulnerabilities and to select appropriate OPSEC measures, i.e., change of procedures, enhanced security, deception, etc.;
- enactment of measures to ensure that all personnel, commensurate with their positions and security clearances, are aware of adversary intelligence threats and understand the OPSEC process;
- annual review and evaluation of the OPSEC procedures to improve OPSEC programs;
- provision for interagency support and cooperation with respect to OPSEC programs.

Heads of executive departments and agencies are also required to advise the National Security Council (NSC) on OPSEC measures required of other departments and agencies in order to achieve and maintain effective operations or activities.

Executive Agent for OPSEC Training

The NSDD assigned the director of the National Security Agency (NSA) as the executive agent for interagency OPSEC training. The executive agent was given the responsibility to assist executive departments and agencies to establish OPSEC programs; develop and provide interagency OPSEC training courses; and establish and maintain an Interagency OPSEC Support Staff (IOSS), whose membership would include as 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.

In order to carry out his NSDD responsibilities, the director, NSA, appointed a director of operations security and established the IOSS. The director of operations security has the responsibility for oversight and support of IOSS activities on behalf of the executive agent. In addition, the director of operations security is responsible for implementation, direction, and oversight of OPSEC within the NSA and the cryptologic community.

The Interagency OPSEC Support Staff

The NSDD stipulates that the IOSS will carry out national-level interagency 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, as required, for the NSC.

The IOSS was established in January 1989 and is located in suburban Maryland, just outside of Washington, D.C. The IOSS is a distinctly interagency organization. The staff comprises individuals from the executive departments and agencies required by the NSDD to provide representation. In addition, other organizations have been invited to assign persons to the IOSS to help provide OPSEC support to their parent organization and as a way to gain valuable OPSEC experience. The IOSS comprises individuals with both OPSEC and various technical expertise and with experience in many different aspects of government activities.

The IOSS operates as a government "consulting firm" providing OPSEC advice and services to executive departments and agencies. It can provide help in the areas of program development, training, briefings, developing reference materials and audio visual aids, and providing or arranging for support to OPSEC surveys and other OPSEC activities. Initially, the IOSS concentrated on assisting organizations in implementing OPSEC programs. The IOSS also developed materials to assist organizations in establishing and maintaining their OPSEC programs. The IOSS sponsors a National

OPSEC Conference, seminars on OPSEC-related subjects, and community-of-interest working groups.

CONCLUSION

The National OPSEC Program was established as a response to the increasing need for and interest in OPSEC by government departments and agencies. Interest has been increasing for three main reasons: (1) OPSEC practitioners have been improving and refining the OPSEC process, making it more useful and easier to apply; (2) there has been a realization of OPSEC's natural potential in nonmilitary as well as military activities; and, most important, (3) there has been a general recognition that adversary intelligence collection capabilities are improving, the vulnerability to exploitation is increasing, and the impact of loss of data is escalating.

In the "information age," indicators, the category of information OPSEC was originally developed to protect, have become more difficult for organizations to control and much easier for adversaries to exploit. The loss of critical information to our adversaries has reached serious proportions and is impacting adversely on government activities. OPSEC has proved to be an essential element in ensuring effective operations of the executive departments and agencies and their supporting contractors.

STATUTORILY EXEMPT