RANGE OPERATIONS GROUP

DOCUMENT 600-11

OPERATIONS SECURITY (OPSEC) GUIDE

WHITE SANDS MISSILE RANGE
REAGAN TEST SITE
YUMA PROVING GROUND
DUGWAY PROVING GROUND
ABERDEEN TEST CENTER
ELECTRONIC PROVING GROUND
HIGH ENERGY LASER SYSTEMS TEST FACILITY

NAVAL AIR WARFARE CENTER WEAPONS DIVISION, PT. MUGU
NAVAL AIR WARFARE CENTER WEAPONS DIVISION, CHINA LAKE
NAVAL AIR WARFARE CENTER AIRCRAFT DIVISION, PATUXENT RIVER
NAVAL UNDERSEA WARFARE CENTER DIVISION, NEWPORT
PACIFIC MISSILE RANGE FACILITY
NAVAL UNDERSEA WARFARE CENTER DIVISION, KEYPORT

30TH SPACE WING
45TH SPACE WING
AIR FORCE FLIGHT TEST CENTER
AIR ARMAMENT CENTER
ARNOLD ENGINEERING DEVELOPMENT CENTER
BARRY M. GOLDWATER RANGE

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION

This page intentionally left blank.

DOCUMENT 600-11

OPERATIONS SECURITY (OPSEC) GUIDE

APRIL 2011

Prepared by

RANGE OPERATIONS GROUP
OPERATIONS SECURITY COMMITTEE

Published by

Secretariat
Range Commanders Council
U.S. Army White Sands Missile Range,
New Mexico 88002-5110

This page intentionally left blank.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

This page intentionally left blank.

PREFACE

This document presents the results of Task ROG-008 "Update to RCC 600-07 Operations Security (OPSEC) Guide" for the Range Operations Group (ROG) in the Range Commanders Council (RCC). Security programs and procedures already exist to protect classified matters. However, information generally available to the public as well as certain detectable indicators 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 OPSEC process promotes operational effectiveness by helping prevent the inadvertent compromise of sensitive or classified U.S. Government activities, capabilities, or intentions.

The OPSEC process is a systematic and proven process that the U.S. Government and its supporting contractors can use to deny potential adversaries access to information about capabilities and intentions of the U.S. Government. The program is implemented by identifying, controlling, and protecting generally unclassified evidence of the planning and execution of sensitive Government activities (Reference a: National Security Decision Directive (NSDD) No. 298).

The RCC gives special acknowledgement for production of this document to:

Author: Mr. Jerry A. Noe
Member Range Operations Group (ROG)
45th Space Wing Operations Security Officer
45th Space Wing (45 OSS)
Patrick AFB, FL 32925-3299
Phone: DSN: 467-6891 Comm: (321) 853-6891
Fax: DSN: 467-7121 Comm: (321) 853-7121
E-Mail: jerry.noe@patrick.af.mil

Please direct any questions to:

Secretariat, Range Commanders Council
ATTN: TEDT-WS-RCC
100 Headquarters Avenue
White Sands Missile Range, New Mexico 88002-5110
Telephone: (575) 678-1107, DSN 258-1107
E-mail wsmrrcc@conus.army.mil

This page intentionally left blank.

ACRONYMS AND INITIALISMS

AF	Air Force
AF SUP	Air Force Supplement
AFDD	Air Force Doctrine Document
AFI	Air Force Instruction
AFOSI	Air Force Office of Special Investigations
AFPD	Air Force Policy Directive
AR	Army Regulation
ATO	Anti-Terrorism Office
AVA	Agency Vulnerability Assessment
CDD	Capability Development Document
CJCS	Chairman, Joint Chiefs of Staff
CJCSI	Chairman, Joint Chiefs of Staff Instruction
CI	Critical Information
CI	Counterintelligence
CIL	Critical Information List
COMINT	Communications Intelligence
COMSEC	Communications Security
CONOPS	Concept of Operations
CONPLAN	Concept Plan
DoD	Department of Defense
DODD	Department of Defense Directive
DODI	Department of Defense Instruction
DODR	Department of Defense Regulation
DTIRP	Defense Treaty Inspection Readiness Program
EEFI	Essential Elements of Friendly Information
ELINT	Electronic Intelligence
EW	Electronic Warfare
EW Ops	Electronic Warfare Operations
FISINT	Foreign Instrumentation Signals Intelligence
FOIA	Freedom of Information Act
FOUO	For Official Use Only
FP	Force Protection
HUMINT	Human Intelligence
IA	Information Assurance
ICD	Initial Capability Documents
IMINT	Imagery Intelligence
IO	Information Operation
InOps	Influence Operation
IOSS	Interagency OPSEC Support Staff
IOTAC	Information Operations Threat Analysis Center
IRD	Initial Requirements Document
IW	Information Warfare
IWU	Information Warfare Unit
JCS	Joints Chiefs of Staff

JP	Joint Publication
JSIVA	Joint Staff Integrated Vulnerability Assessments
MASINT	Measurement and Signature Intelligence
MCTL	Military Critical Technologies List
MDVA	Multi-disciplined Vulnerability Assessment
MI	Military Intelligence
MILDEC	Military Deception
MRTFB	Major Range and Test Facility Base
NASA	National Aeronautics and Space Administration
NSC	National Security Council
NIPRnet	Nonsecure Internet Protocol Routing Network
NSDD	National Security Decision Directive
NSTISSI	National Security Telecommunications and Information Systems Security Instruction
NW Ops	Network Warfare (NW) Operations
OPNAV	Office of the Chief of Naval Operations
OPLAN	Operations Plans
OPORD	Operations Orders
OPSEC	Operations Security
ORM	Operational Risk Management
OSINT	Open Source Intelligence
OWG	OPSEC Working Group
PA	Public Affairs
PM	Program Manager
PPP	Program Protection Plan
PSYOP	Psychological Operations
RA	Risk Assessment
RDT&E	Research, Development, Test, and Evaluation
ROG	Range Operations Group
SAP	Special Access Program
SAV	Staff Assistance Visit
SBU	Sensitive But Unclassified
SD	Security Detachment
SecFor	Security Forces
SECNAVINST	Secretary of the Navy Instruction
SI	Senior Intelligence
SIGNINT	Signal Intelligence
SOW	Statement of Work
RFP	Request for Proposal
TAC	Threat Analysis Center
TECHINT	Technical Intelligence
TMAP	Telecommunications Monitoring and Assessment Program
TTP	Tactics, Technologies, and Procedures
TWG	Terrorism Working Group (formerly Threat Working Group)

CHAPTER 1

INTRODUCTION

1.1 Background

Operations Security (OPSEC) involves a series of steps to examine the planning, preparation, execution and post execution phases of any activity across the entire spectrum of military actions and operational environments. OPSEC analysis provides decision-makers with a means of weighing how much risk they are willing to accept in specific operational circumstances in the same way as Operational Risk Management (ORM) allows Commanders to assess risk in mission planning. In fact, OPSEC can be referred to as information risk management.

The OPSEC process will be employed with other complementary Information Operation (IO) activities to obtain maximum effectiveness. Commanders and their planners should utilize all capabilities within information operations, including OPSEC, in a synchronized effort to influence the perceptions and affect decision-making of an adversary. For example, a known OPSEC vulnerability may be used to deliver a deception message or psychological operations theme instead of simply correcting or mitigating the vulnerability. In this case, the use of the discovered vulnerability would be considered application of the appropriate OPSEC measure.

1.2 Responsibilities and Authorities

Operational effectiveness is enhanced when Commanders and other decision-makers apply OPSEC from the earliest stages of planning. A detailed discussion on OPSEC responsibilities and authorities is provided at Appendix A.

1.3 Scope

The OPSEC process is an integral process of force protection to help protect Service members, civilian employees, family members, facilities, and equipment at all locations and in all situations. Force protection relies heavily on OPSEC as a means of denying targeted information to terrorists and other adversaries. Since force protection safeguards an organization's most precious asset (i.e. people), it is critical that OPSEC be applied throughout all organizations.

The OPSEC is also a process and capability within IO. The IO is the integrated employment of three operational elements:

a. Influence operations (InOps)
b. Electronic warfare (EW) operations (EW Ops)
c. Network warfare (NW) operations (NW Ops).

The purpose of InOps is to influence, disrupt, corrupt, or usurp adversarial human or automated decision-making while protecting our own decision-making capabilities. Influence Operations employ core military capabilities of psychological operations (PSYOP), OPSEC,

military deception (MILDEC), counterintelligence (CI) operations, public affairs (PA) operations, and counter-propaganda operations to affect behaviors, protect operations, communicate Directors' and Commanders' intentions and project accurate information to achieve desired effects across the cognitive battle space. OPSEC protects friendly operations and efforts in order to influence the adversary's behavior.

The OPSEC should be closely coordinated with the other security disciplines. To ensure that all aspects of sensitive activities are protected, each Service has regulations that specifically apply to security disciplines. These disciplines include physical security, acquisition security, industrial security, information security or safeguarding classified information, information systems security or transmission of information via the Internet and electronic mail (e-mail) management and use, antiterrorism/force protection, personnel security, foreign disclosures (visits or requests for information from foreign representatives). Also, public affairs policies and procedures for each Service require a security review prior to disclosure of any information to the public. Information related to technologies provided by other Department of Defense (DoD) agencies, as well as national laboratories and ranges, also requires coordination with the system developer/system owner/program manager and other affected agencies prior to public disclosure. The primary focus of OPSEC analysis is to deny potential exploitation of open sources and observable actions. These sources are generally unclassified and, consequently, more difficult to control. A list of related Service security regulations is provided in Table 3-1 of this document.

1.4 OPSEC Definition

The OPSEC is a process of identifying, analyzing, and controlling critical information indicating friendly actions attendant to military tactics, techniques, and procedures (TTPs), capabilities, operations, and other activities to:

a. Identify actions that can be observed by adversarial intelligence systems.
b. Determine what indicators adversarial intelligence systems might obtain that could be interpreted or combined to derive critical information in time to be useful to adversaries.
c. Select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation.

CHAPTER 2

THE OPSEC PROCESS

2.1 Overview

Utilizing OPSEC is a process and not a collection of specific rules and instructions that can be applied to every operation. OPSEC must be closely integrated and synchronized with other Information Operation (IO) capabilities and all aspects of the protected operations.

OPSEC is accomplished with a five-step process. Although these steps are normally applied in a sequential manner during deliberate or crisis action planning, dynamic situations may require any step to be revisited at any time. The OPSEC process is therefore cyclical in nature. The five steps are:

Step 1: Identification of critical information (CI) and indicators.
Step 2: Threat assessment.
Step 3: Vulnerability analysis.
Step 4: Risk assessment.
Step 5: Application of appropriate OPSEC measures and countermeasures.

2.2 Step 1: Identification of Critical Information (CI) and Indicators

Critical information is information about friendly (U. S., allied, and/or coalition) activities, intentions, capabilities, or limitations that an adversary seeks in order to gain a military, political, diplomatic, economic, or technological advantage. Another term for CI is Essential Elements of Friendly Information (EEFI). Such information, if revealed to an adversary prematurely, may prevent or complicate mission accomplishment, reduce mission effectiveness, or cause loss of lives or damage to friendly resources. Critical information may also be derived from seemingly unrelated elements of information known as indicators. The product of the first step in the OPSEC process is the development of a Critical Information List (CIL). The sample CIL at Table 2-1 is not all-inclusive, but contains examples of indicators that can provide adversaries with information about our capabilities and intentions.

The goal of OPSEC is to identify information and observable activities relating to mission capabilities, limitations and intentions in order to prevent exploitation by our adversaries. OPSEC methodology provides a systematic analysis of our operations and behavior from an adversary's perspective, thereby assessing how vulnerabilities could be exploited. Information that adversaries need to achieve their goals constitutes critical information about our operations or programs. By identifying and protecting this critical information, the OPSEC process becomes a positive, proactive means by which adversaries are denied an important advantage.

OPSEC provides a method of identifying our critical information and denying or controlling an adversary's access to that information. OPSEC enables friendly force information superiority by neutralizing adversary information collection activities.

TABLE 2-1. SAMPLE CRITICAL INFORMATION LIST (CIL)

- Work schedules
- Shipping requests or announcements
- Meeting minutes or notes
- Various reports (monthly, annual, etc.)
- Scope-of-work orders
- Staffing reports
- Unusual occurrence reports
- Purchasing requests
- Travel requests/trip reports
- Project units/blueprints
- News releases
- Progress reports
- Published articles
- Corporate newsletters
- Emergency plans
- Budget or financial documentation
- Employee suggestions
- Standard Operating Procedures
- Environmental Impact Statements
- Position vacancy announcements
- Operating manuals
- Safety reports
- Quality assurance notes
- Information contained on home pages
- Stereotyped activities (test schedules, range schedules, test preparations, range closures, etc.)
- Increased levels of communications
- Transportation arrangements
- Distinctive emblems or logos, marking on personnel, equipment, and supplies
- Prepositioning and establishment of logistic bases.
- In most cases, unclassified information identified as critical is described as "Sensitive but Unclassified."

2.2.1 OPSEC Indicators. OPSEC indicators are those friendly actions and information that adversary intelligence efforts can potentially detect or obtain and then interpret to derive friendly critical information. Indicators may be classified or unclassified. Indicators are activities that can be heard, observed, or imagined, which could compromise mission critical information. Indicators obtained by an adversary or competitor could result in adversary knowledge or actions harmful to friendly intentions. Indicators include such things as personnel or material actions and movements that can be observed, including public releases, conversations or documents, and habitual procedures when conducting a given type of operation or test. All detectable indicators that convey or infer critical information must be identified and protected if determined vulnerable.

2.2.2 OPSEC Working Group (OWG). Critical information is best identified by the individuals who are managing and developing the test item or responsible for the planning and execution of the unit's mission. An OWG comprised of members who are managing and developing the test item or are responsible for the planning and execution of unit mission can most effectively accomplish this task. Once a CIL is developed, Commanders must approve the list and then ensure their critical information is protected and controlled.

2.2.3 Early Identification. Critical information should be identified at the earliest possible time, preferably during the planning phases of an acquisition/development process or operation.

Subordinate and supporting organizations should be notified of critical operational information so they too can protect the information and any associated indicators.

2.2.4 Revising the Critical Information List (CIL). The organizational CIL should be revised as required to reflect changing mission/operational requirements. While categories of critical information are fairly stable, specific items of information are normally only critical for a prescribed period. The need to control or protect specific items of information will change as the mission/operation progresses or the threat changes.

2.2.5 Unclassified or Classified? Critical information can be unclassified or classified. Unclassified critical information can be labeled as Sensitive but Unclassified (SBU) or For Official Use Only (FOUO). In most cases, unclassified information identified as critical is described as SBU.

2.3 Step 2: Threat Assessment

2.3.1 Current Threat Information. Current threat information is extremely important in developing appropriate OPSEC measures. The threat assessment includes identifying potential adversaries and their associated capabilities, limitations, and intentions to collect, analyze and use critical information and OPSEC indicators.

2.3.2 Counterintelligence (CI) Studies. The DoD and other federal agencies produce Counterintelligence (CI) studies. They analyze multi-disciplinary intelligence to evaluate threats from foreign intelligence Services. Security offices/detachments produce local counterintelligence and criminal threat assessments on an annual basis. These assessments provide valuable input for OPSEC program decisions, thereby helping protect both personnel and resources. Security offices/detachments may also produce focused counterintelligence studies when requested. Threat data can also be obtained through various other sources including the Information Operations Threat Analysis Center (IOTAC) and local intelligence units upon request.

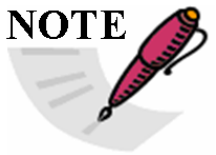
2.4 Step 3: Vulnerability Analysis

2.4.1 Existence of Vulnerability. An OPSEC vulnerability exists when an adversary is capable of collecting an OPSEC indicator, analyzing it, and then acting quickly enough to affect their decision making process. Vulnerabilities are weaknesses that reveal critical information through indicators that have been collected and analyzed. Guidelines for identifying vulnerabilities are at Appendix B.

2.4.2 Following Appropriate Unit Capabilities. The vulnerability analysis should include consideration of the following:

a. Human Intelligence (HUMINT). The use of personnel to gain information that is often inaccessible by other collection means. This activity can be legal (e.g., elicitation at a technical conference) or clandestine (e.g., disgruntled employee, spying)

b. Imagery Intelligence (IMINT). From visual photography, infrared sensors, lasers, electro-optics, and radar sensors that can operate from land, sea, air, and space platforms.
c. Signals Intelligence (SIGNINT). From Communications Intelligence (COMINT), Electronics Intelligence (ELINT), and Foreign Instrumentation Signals Intelligence (FISINT).
d. Measurement and Signature Intelligence (MASINT). From qualitative and quantitative analysis of data derived from specific technical sensors.
e. Open Source Intelligence (OSINT). From information of potential intelligence value available to the general public, such as the Internet, television, newspapers, magazine articles, and brochures.
f. Technical Intelligence (TECHINT). From the exploitation of captured or otherwise obtained foreign materiel and equipment.



Two effective tools in protecting critical information are the document review process and the personnel interview process. These tools and measures associated with them are described in Appendix O and P.

2.5 Step 4: Risk Assessment

Risk assessment is the measure of harm or adverse impact that a vulnerability or combination of vulnerabilities may cause if exploited by an adversary. Whether the vulnerability will be successfully exploited depends on the intelligence capability and intent of the adversary, (i.e., the existence of the threat and the opportunity to exploit the vulnerability). By considering all identified vulnerabilities, a subjective measure of the likelihood of success can be determined. The likelihood of successful exploitation and the potential adverse impact can then be considered in order to develop a subjective measure of risk. A Risk Assessment (RA) should consider the following:

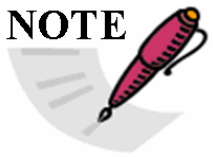
a. The OPSEC program managers and coordinators, in concert with other planners and with the assistance of intelligence and counterintelligence organizations, will provide risk assessments and recommended actions to senior decision-makers and Commanders. Commanders must then decide whether to employ recommended OPSEC measures.
b. Risk assessment involves an estimate of an adversary's capability to exploit a vulnerability, the potential effects that such exploitation will have on operations, and a cost-benefit analysis of possible methods to control the availability of critical information to the adversary.
c. The guiding principles of ORM, managing all dimensions of risk to maximize mission effectiveness and sustain readiness, must be applied to OPSEC. Applying these principles will ensure that unnecessary OPSEC risks are avoided and that OPSEC risks are accepted when the cost of mitigation outweighs the benefit. Costs and benefits are likely to be operational versus monetary.

2.6 Step 5: Application of Appropriate OPSEC Measures and Countermeasures

2.6.1 OPSEC Measures. Recommended OPSEC measures are designed to preserve the integrity of military information and capabilities by preventing adversarial exploitation of critical information. The OPSEC measures are employed to mitigate or exploit vulnerabilities to the protection of critical information. The OPSEC measures help control critical information by managing the raw data and enhancing friendly capabilities by increasing the potential for surprise and effectiveness of friendly military forces and weapon systems.

The OPSEC measures, and countermeasures, (see Appendix C) consist of a combination of physical and IO capabilities that counter an adversary's ability to gain and exploit friendly information. These measures must be implemented as part of an overall IO effort to influence the adversary's perceptions and situational awareness. OPSEC measures fall under the following three general categories:

a. Preventing the adversary from detecting critical information and indicators. The objective is to eliminate or disrupt an adversary's activities to effectively gather information on indicators or to effectively exploit our vulnerabilities.
b. Providing alternative deceptive interpretations of critical information and/or indicators. Sometimes it may not be cost-effective to control actions that reveal critical information or become the source of an OPSEC indicator. In these circumstances, OPSEC measures are aimed at influencing and affecting the adversary's ability to properly interpret the information.
c. Attacking the adversary's collection system. This category of OPSEC measures is to use IO capabilities or kinetic operations to attack an adversary's intelligence collection system and thus eliminate or reduce their ability to obtain critical information. Examples of this include electronic attack against technical collection platforms and physical destruction of intelligence fusion and analysis centers.



All OPSEC measures must be synchronized with other components of Information Operations (IO). These measures must be implemented as part of an overall IO effort to influence the adversary's perceptions and situational awareness. Care must be taken so that OPSEC measures do not become unacceptable indicators themselves.

2.6.2 OPSEC Countermeasures and the Implementation Process (see Appendix C).

a. Countermeasures. Countermeasures should be based on vulnerabilities and indicators. Once the possible countermeasures have been identified, a decision must be made to select those most suitable for implementation. The following appropriate unit factors should be considered:
   (1) What is the benefit, or the effect of the countermeasure on reducing risk to the mission or asset?
   (2) What is the cost of the countermeasure in terms of dollars, time to implement, human and technical resources, duration that it will remain effective, and potential adverse affect on mission accomplishment?

(3) Will the countermeasure create another exploitable indicator?

b. Countermeasure Implementation Process. Countermeasures are the measured responses to identified threats. Measures are general responses to pervasive but not focused threats. As an example, the threat of wire-tapping could be unfocused in your area, but effective communications security, use of secure telephones, and a robust Telecommunications Monitoring and Assessment Program (TMAP) prevents undetermined pervasive threats from degrading operations. Prior to implementation, the following actions need to occur.

(1) A countermeasure should be carefully evaluated to ensure that it does NOT create OPSEC issues by implementing the countermeasure itself. Countermeasures must also be evaluated based on the cost to execute and the impact on mission operations.

(2) Before countermeasures are implemented, it is necessary to brief senior management on the associated cost, operational impact, and benefits. Senior management must "buy into" the proposed countermeasures in order to ensure effective and consistent application of the countermeasure with full support from all involved parties.

(3) A specific countermeasure that is highly recommended in the management and destruction of unclassified operationally sensitive documents is the use of either a shredder with shred size of 3/8 by 1.5 inches or less combined with the maximum use of a secured recycle process (an example of this process is provided in Appendix M. The secured recycle process is highly recommended due to EPA recycle requirements detailed in *USC 40 CFR 246.200-1* ensuring maximum recycle, as required by federal regulations, without sacrificing OPSEC integrity.

(4) A metric that can be used to measure the effectiveness of the document management and destruction process is periodic trash receptacle inspections. A safety and environmental health approved example process is provided at Appendix N.

2.7 OPSEC Tools (Assessments, Surveys, and Reviews)

2.7.1 Purpose. The OPSEC assessments, surveys, and reviews are accomplished to gauge the overall health of the OPSEC program, to examine actual practices and procedures, and to identify new or previously undiscovered vulnerabilities. Commanders, Program Managers (PMs), and coordinators use assessment results within the risk management process to implement protective measures and improve the OPSEC posture of the unit/activity.

2.7.2 Scheduling. The PMs will coordinate with their higher headquarters and subordinate units to schedule assessments and surveys. The PMs will then validate and prioritize their units and supporting elements based on a priority system taking into account the unit's mission criticality, threat (based on inputs from intelligence and counterintelligence sources) and operations tempo.

2.7.3 Types of Assessments. The nature of the assessment depends on the unit's mission criticality, availability of resources, and Commander guidance. There are several types of

assessments available to OPSEC PMs or coordinators to gauge the effectiveness of their program. Some of the assessment types are briefly discussed below and charted in Table 2-2.

a. Program Self-Assessment. Unit PMs and coordinators will conduct annual self-assessments to ensure the health of their program, evaluate compliance with applicable policies, and to identify shortfalls and vulnerabilities. Appendix D contains a sample self-assessment checklist that can be modified to suit specific unit/activity needs, and used in conjunction with directive/regulatory, self-evaluation tools/documentation.
b. Web Risk Assessment. Web risk assessment includes conducting ongoing OPSEC analysis of content and data residing on publicly accessible and Nonsecure Internet Protocol Routing Network (NIPRnet) websites. Web risk assessment follows guidance contained within Air Force Instruction 33-129 (AFI 33-129), *Web Management and Internet Use*, and AFI 33-219, *Telecommunications Monitoring and Assessment Program (TMAP)*, or Information Assurance (IA) or Communications Security (COMSEC) guidance provided for the Army and the Navy for their web sites or other telecommunications. Web risk assessment is an integral portion of TMAP. The goal of Web risk assessment is to improve the OPSEC posture and identify critical information available for adversary exploitation. Web risk assessment reviews and evaluates findings, reports to the unit for correction, and forwards results to the IO Threat Analysis Center (TAC) for fused analysis and dissemination.
c. Telecommunications Monitoring and Assessment Program (TMAP). The TMAP involves the collection and analysis of unsecured and unprotected voice, fax, data (networks and wireless devices), and other electronic transmissions or communications systems to evaluate an organization's OPSEC posture and determine the amounts and types of information available to adversary collection entities. Telecommunications monitoring is accomplished only within certain legal parameters and may only be performed by authorized agencies as outlined in the organizations directives/regulations. Telecommunications monitoring is normally conducted upon request of an appropriate authority (Director or Commander), provided assets are available. The analysis and recommendations are formally reported to the requesting authority. Telecommunications monitoring can be conducted as part of a survey, a Multi-disciplined Vulnerability Assessment (MDVA), or a stand-alone assessment.
d. Staff Assistance Visit (SAV). A SAV conducted by higher headquarters or for subordinate units/organization should be used to enhance the overall OPSEC Program and to provide guidance to PMs/Coordinators as required. SAVs also identify and share "best practices" throughout their respective agency.
e. Multi-disciplinary Vulnerability Assessment (MDVA). The MDVA is one type of OPSEC Vulnerability Report that identifies a possible disclosure of information of identifies an OPSEC indicator. Additional information is at Paragraph 3.4.

TABLE 2-2. TYPES OF OPSEC ASSESSMENTS AND THE OPSEC SURVEY

Assessment Type	Purpose	Methodology	Frequency	Request Procedures	Reporting
Program Self-Assessment	-Program Health -Policy Compliance -Shortfalls	Self-Assessment by unit OPSEC PM/Coordinator	Annual	N/A	OPSEC PM/Coordinator reports to Unit and Up Channel to HHQ PM
Web Risk Assessment	OPSEC review of unit website	Website reviewed as part of TMAP	Biennial	Unit requests through HHQ PM	Report to Unit
Electronic Monitoring and Assessment (E.G. – TMAP)	ID vulnerabilities	Collect and analyze communications	Biennial	Unit requests through HHQ PM	Report to Unit
SAV	- Policy Compliance - Shortfalls - Provide Guidance	OPSEC PMs assess subordinate units (if collocated)	As required	N/A	Report to subordinate Unit and OPSEC PM or Coordinator
Multi Disciplinary Vulnerability Assessment (MDVA)	Assess application of influence operations	IO Red Team simulates IO threats to identify vulnerabilities, operational impacts, & exercise threat response procedures	As required	Installation CC or Director requests through OPSEC PM	Out-brief & report to installation CC or Director
OPSEC Survey	Assess unit OPSEC practice and procedures	Team analyzes documentation and interview personnel for: - IO Threat - Critical Information - Operational Procedures - Potential Indicators & Vulnerabilities	At least every three years	Command Survey: Done in-house Formal Survey: Unit requests through OPSEC PM	Out-brief and report to Unit

2.7.4. OPSEC Surveys. The OPSEC survey is a systematic process to examine the actual practices and procedures employed by an activity or operation to achieve its goals. The methodology consists of using a team to look at an activity through the eyes of an adversary to determine if critical information may be inadvertently disclosed through the performance of normal organizational functions. The primary purpose of the review is to evaluate and improve organizational effectiveness and control the vulnerabilities of friendly actions or information. Survey requirements of subordinate units are based on criticality of mission. Two types of surveys are formal and in-house.

a. Formal Survey. A formal survey concentrates on activities that cross command lines, and requires a survey team composed of members from inside and outside the command.
b. Command (In-house) Survey. An in-house survey concentrates on activities within the particular agency or unit, and is performed only by in-house personnel. The in-house survey is the more common of the two survey methods and can be conducted throughout all organizational levels.

Procedures for each of the two survey types (formal and in-house) are unique due to the nature of the information requiring control, the adversary collection capability, and the environment of the activity to be surveyed.

To assist in performing either type of survey, the following guidelines are provided at the following appendices:

Appendix	Title
D	Self Assessments OPSEC Inspection Checklist (Example).
E	OPSEC Survey Planning Worksheet.
F	OPSEC Interview Checklist.
G	OPSEC Survey Report Format (Sample).
H	OPSEC Review of Paper/Presentation (Example).

2.8 Arms Control OPSEC Planning

The Defense Treaty Inspection Readiness Program (DTIRP) offers assistance and guidance in making facilities compliant with arms control treaties and agreements. The program's focus is to ensure readiness through awareness by augmenting traditional OPSEC procedures to guarantee maximum security. Specifics of DTIRP's arms control OPSEC planning can be found at Figure 2-1.

Note: Figure 2-1 is an extract from the:
Defense Treaty Inspection Readiness Program Arms Control OPSEC Brochure:

International arms control treaties and agreements are important tools for reducing the threats posed by conventional, chemical, biological, and nuclear weapons. Many of these agreements contain provisions allowing the States Parties to verify compliance. Compliance verification activities often include:

• submitting data declarations to other States Parties or to an international treaty implementation organization; and/or
• hosting and conducting on-site inspections, monitoring missions, and observation overflights.

A wide range of Department of Defense (DoD) facilities, as well as defense contractor and commercial sites are impacted by these activities. Clearly, the physical presence of a foreign inspection team during an on-site inspection creates unique security challenges that cannot be met by traditional operations security (OPSEC) measures alone. For this reason, the U.S. Government has developed the arms control OPSEC process, which augments traditional OPSEC measures.

As shown below, two new steps have been added to the Measure of Success traditional OPSEC process: susceptibility and probability.

Measure of Success: Demonstrate treaty compliance while protecting national security, proprietary, and other sensitive information.

Arms Control OPSEC Process

1. Identify sensitive information
2. Determine susceptibility*
3. Understand the threat
4. Determine vulnerability
5. Assess risk of compromise
6. Assess probability*
7. Develop and implement countermeasures

*Arms control OPSEC step

Arms control OPSEC is a systematic 7-step process for identifying sensitive information and unclassified indicators, assessing risks, and developing appropriate and cost effective security countermeasures to protect national security, proprietary, and other sensitive information.

The arms control OPSEC process augments traditional OPSEC methods to help facility staff and U.S. Government personnel evaluate and prepare for the unique security challenges associated with conducting on-site inspection activities. Traditional methods primarily rely on a layered system of security fences and procedures. These methods restrict access and keep potential threats out of, and away from, sensitive information and areas. However, during on-site inspection activities, the inspection team will generally have access to a number of areas and have the right to obtain certain types of information.

When selecting security countermeasures, it is important to consider a number of factors. First, security countermeasures should be cost effective— if the cost of implementing a countermeasure is greater than the value of the information being protected, the countermeasure provides no benefit. Countermeasures should also be as transparent as possible to avoid attracting unwelcome attention from the inspection team. Finally, appropriate countermeasures should be able to protect sensitive information while also allowing the inspection team to verify that the item being protected is not a compliance concern.

Over the past two decades, DoD, DoD Components, and facility personnel have developed and applied the arms control OPSEC process to successfully host on-site inspections. Many lessons have been learned about the importance of advance planning, training, teamwork, and effective communications. Specifically, these lessons include the following: • conduct treaty and inspection readiness training for appropriate personnel—this may include classroom briefings, exercises, and mock inspections;

• conduct a vulnerability assessment;
• anticipate the inspection team's requirements, requests, and capabilities;
• identify appropriate ways of accommodating the inspection team's legitimate needs;
• develop cost-effective security countermeasures;
• plan inspection routes within buildings and throughout the facility;
• prepare a written plan for all inspection-related activities;
• ensure that facility staff are aware of and ready to operationalize their responsibilities during inspection activities; and
• maintain an up-to-date communications plan to quickly contact key personnel when the facility is notified of an impending inspection.

To obtain more information about the arms control OPSEC process, treaty provisions, vulnerability assessments, and the application of appropriate security countermeasures, contact the DTIRP Outreach Program Coordinator at 1-800-419-2899 or by email at dtirpoutreach@dtra.mil, your local Defense Security Service (DSS) Industrial Security Representative, or your government sponsor. Additional DTIRP products are available on the DTIRP website at: http://dtirp.dtra.mil.

Figure 2-1: Extract from Arms Control OPSEC Brochure

This page intentionally left blank.

CHAPTER 3

RANGE COMMANDERS COUNCIL (RCC) OPSEC PROGRAM

3.1 Purpose

All organizations should integrate OPSEC into their planning and develop OPSEC plans to ensure critical information and indicators are identified. Although the OPSEC program helps Commanders and Directors make and implement decisions, the decisions are the responsibilities of the Commanders and Directors. Leaders must understand the risk to the mission and then determine which OPSEC measures are required. The RCC should integrate OPSEC into the following areas:

a. Strategy.
b. Operational and tactical planning and execution.
c. All support activities.
d. All contingency, combat, and peacetime operations and exercises.
e. Communications-computer architectures and processing.
f. Weapons systems research, development, test, and operation (RDT&E).
g. Specialized training.
h. Inspections.
i. Acquisition and procurement.
j. Professional education.

3.2 Roles and Responsibilities

3.2.1 OPSEC PMs or OPSEC Officers. The OPSEC PMs or OPSEC Officers and alternates will be assigned at the appropriate unit level (or above) as determined by directive/command. Organizations must appoint an OPSEC PM or Officer and an OPSEC Alternate in writing. The OPSEC PM or Officer can be at any organizational level the Commander or Director deems appropriate. For example, an appropriate unit PM may actually be assigned at the Operations Group level, but perform OPSEC PM duties in direct support of the entire organization. Letters of appointment must be forwarded to respective higher headquarters and to OPSEC PMs as appropriate. The respective Commander or their designee will sign appointment letters. Units below that level that do not have OPSEC PMs must assign an OPSEC Coordinator and Alternate to work with OPSEC PMs. OPSEC PMs at the Directorate or division level should be assigned for a minimum of 18 months. The OPSEC PM requires a security clearance appropriate to the mission and function of the organization, but not less than "Secret." OPSEC PMs should have access to the Secure Internet Protocol Routing Network (SIPRNet) to access OPSEC Advisory Reports. All OPSEC PMs should establish NIPRNet and SIPRNet accounts. Host installation OPSEC PMs will coordinate OPSEC with tenant unit OPSEC PMs and/or Coordinators. Tenant OPSEC PMs and Coordinators will closely coordinate and integrate with host OPSEC initiatives; however, administrative oversight of the tenant unit's program still resides with their respective parent organization. If the host organization has an OPSEC working group, the tenant

unit PM or Coordinator will seek representation in it. If possible, OPSEC PMs should not have any other duties.

3.2.2 OPSEC PM Duties. The OPSEC PM duties include, but are not limited to:

a. Develop, coordinate, and manage the OPSEC Program implementation throughout their organization.
b. Incorporate OPSEC into organizational plans, exercises, activities, and command-to-command agreements.
c. Ensure OPSEC is incorporated into organizational/program plans, exercises, and activities through the unit's planning process. Forward lessons learned to appropriate depositories.
d. Oversee development and implementation of the Commander's OPSEC policy and CIL.
e. Develop procedures to ensure critical information, CILs, and OPSEC indicators are controlled.
f. Ensure OPSEC reviews are conducted on all web pages annually or prior to the information being placed, updated, or modified on the web page.
g. Ensure OPSEC considerations are included in all public release review and approval process for the publishing or releasing of information to or that may be viewed by the public; i.e. technical papers/articles, brochures, base newspapers, safety magazines, flyers, web pages, television interviews and information for news articles.
h. Ensure OPSEC reviews consider the proliferation of internet/web-based bulletin boards and web logs (Blogs), and evaluate the risk presented by web content in annual OPSEC assessments/reports (see Appendix I). Ensure OPSEC is integrated into Information Operations, Influence Operations, and other supporting capabilities.
i. Provide management, development, and oversight of appropriate OPSEC training and conduct training as required.
j. Ensure annual OPSEC self-assessments are conducted (to include subordinate units) and results forwarded as required by the governing Service regulation each year.
k. Chair OPSEC Working Groups (OWG) consisting of appropriate security disciplines and applicable supporting organizations.
l. Coordinate and facilitate OPSEC assessments in accordance with paragraph 2.7.
m. Submit OPSEC vulnerability reports in accordance with Paragraph 3.4.1.
n. Ensure OPSEC is integrated into all acquisition programs and contractor support documents/agreements.
o. Conduct Staff Assistance Visits (SAV) to all subordinate units as required or requested.
p. Serve as focal point for OPSEC support capabilities.

3.2.3 OPSEC Coordinators. The OPSEC Coordinators and OPSEC Alternates will be assigned for each subordinate unit under Directorate, division, unit/appropriate unit or appropriate unit equivalent level. Letters of appointment must be forwarded to the respective higher headquarters OPSEC PM. The respective Commander or Director will sign appointment letters. All OPSEC Coordinators will maintain an appropriate clearance, but a minimum level of Secret is required. If possible, OPSEC Coordinators should not have any other

duties. Tenant unit OPSEC Coordinators will closely coordinate and integrate with host OPSEC initiatives; however, administrative oversight of the tenant unit's program still resides with their respective parent organization. If the host has an OPSEC Working Group (OWG), the coordinator should seek representation in it.

3.2.4 OPSEC Coordinator Duties. The OPSEC Coordinator duties include, but are not limited to, the following:

a. Develop, implement, and distribute commander's OPSEC policy and critical information list. Review periodically for currency and update as necessary.
b. Incorporate OPSEC into organizational plans, exercises, and activities.
c. Submit lessons learned from operations and exercises per individual Service's guidance and to the OPSEC PM as appropriate.
d. Oversee development and implementation of Director's or Commander's OPSEC policy and CIL.
e. Develop procedures to ensure critical information and OPSEC indicators are identified and controlled.
f. Ensure OPSEC reviews are conducted on all web pages annually or prior to the information being placed, updated, or modified on the web page.
g. Conduct OPSEC reviews of information submitted for publication or release to the public; i.e. base newspapers, safety magazines, flyers, web pages, television interviews information for news articles.
h. Provide management of unit's OPSEC training and ensure the performance of initial OPSEC training upon arrival of newly assigned personnel and annual refresher training thereafter.
i. Conduct and report annual OPSEC self-assessments to respective Directorate, division, unit/appropriate unit or higher headquarter OPSEC PM as required by the governing Service regulation each year.
j. Participate in OPSEC Working Group as required.
k. Utilize assessment results to correct discovered vulnerabilities and aid organization OPSEC awareness efforts.
l. Submit OPSEC vulnerability reports as required.
m. Integrate OPSEC into all acquisition programs, contractor support documents, and the Universal Documentation System or equivalent.
n. Coordinate with appropriate organizations and senior leadership to resolve/mitigate Web Risk Assessment, TMAP, MDVA, and other OPSEC assessment findings as required.
o. Serve as the unit focal point for OPSEC support capabilities.

3.2.5 OPSEC Planners. The OPSEC planners are personnel who have received specialized planning training (i.e. IO Integration Course, Field Training) to incorporate OPSEC into all functional areas of plans. OPSEC Planners normally reside within the Information Warfare Unit (IWU) construct. OPSEC Planners can also function as part of IO Team.

3.2.6 The OPSEC Working Group (OWG). An OWG will be established at the appropriate unit level. In addition, an ad-hoc OWG should be established for any large-scale operation or

exercise. At appropriate unit level, the OPSEC PM will chair the OWG and report directly to the Commander or Director. The OWG will ensure the timely and efficient review of activities and future plans. The OWG will also integrate OPSEC into all organization planning and operational processes. The OWG composition will vary, depending on various projects or activities being performed. At a minimum, the OWG should include a representative from each exercise or operation, as well as any direct units associated with an exercise or operation. Recommended members include:

a. The Military Deception (MILDEC) Officer.
b. The Psychological Operations (PSYOP) Officer.
c. Senior Intelligence (SI) Officer.
d. Public Affairs (PA) Officer.
e. Force Protection Officer.
f. Information Assurance Officer.
g. Local Air Force (AF) Office of Special Investigations (AFOSI), Service equivalent, or Military Intelligence/Security Detachment.
h. All subordinate OPSEC Coordinators.

The OWG Force Protection member may be either a representative from the organizational Anti-Terrorism Office (ATO) or installation Security Forces (SecFor). The OWG should complement installation anti-terrorism working groups (formerly Threat Working Groups), force protection working groups, and critical infrastructure working groups.

3.3 Training and Awareness

3.3.1 Purpose. Initial and annual OPSEC training provides personnel (military and civilian) with general knowledge of the OPSEC process. Contractors who have access to mission critical information will also receive the same training, or equivalent, as directed in contractual documentation. Training ensures that personnel and supporting contractors understand their individual responsibilities, realize the positive benefits of proper OPSEC and gain a greater appreciation of how the organization uses OPSEC measures to minimize the exploitation of critical friendly information. Formal OPSEC training for those assigned as PMs or Coordinators is accomplished through in-depth training designed to ensure proper management and execution of organizational OPSEC programs. This training can be obtained through the Interagency OPSEC Support Staff (IOSS), United States Air Force (USAF) Information Warfare Center, or equivalent programs developed and sponsored by the individual Services.

3.3.2 OPSEC Training is a Continuing Requirement. Training must be provided to personnel (military and civilian) upon their initial entrance/accession into the work force and upon assignment to new organizations. Contractors must ensure employees receive OPSEC training within the time specified in the contract; the time should not exceed 90 days of initial assignment

to a contract with OPSEC requirements. OPSEC PMs and Coordinators will track and document the completion of training for all military, civilian, and contractor personnel. General guidelines for this training follow:

a. Initial training will provide a brief overview of the OPSEC process, the importance of understanding critical information, and the general adversary threat.
b. Unit-specific OPSEC education will be provided as part of in-processing for all new personnel and before individuals receive access to mission critical information. The purpose of unit OPSEC education is to ensure personnel are familiar with potential threats related to the unit, critical information for the mission it supports, job specific OPSEC indicators, and the OPSEC measures they will execute. Briefings to new personnel should include duty related critical information, the intelligence threat to the mission supported and individual responsibilities. Refresher training must include, as a minimum, updated threat information, changes to critical information, and new procedures, and/or OPSEC measures implemented by the organization.
c. OPSEC Training Documentation. All unit OPSEC Coordinators will track initial and refresher training and report training metric results to respective Higher Headquarters (HHQ) OPSEC PM for inclusion in their annual OPSEC self-assessment report (Appendix D).

3.3.3 OPSEC Training Requirements for PMs and Coordinators.

a. Formal OPSEC training is the required level of training for all persons designated as:
   (1) OPSEC PMs at Directorate or appropriate unit-level and above.
   (2) IO Red Team members who conduct MDVAs.
   (3) Those who conduct formal OPSEC surveys and IG inspections.
b. OPSEC PMs should complete formal Service sponsored or accepted OPSEC training within 90 days of appointment; examples include the DoD OPSEC course available through the Interagency OPSEC Support Staff (IOSS), the Army OPSEC Officer's Course, or equivalent courses. OPSEC PMs and OPSEC planners at the Directorate or unit/appropriate unit level should be scheduled to receive in-residence formal training within 90 days of the assignment. Coordinators below unit level are strongly encouraged to attend formal OPSEC training; however, coordinators below Directorate or unit appropriate unit-level should seek training directly from their next level PM. PMs must maintain general awareness of current OPSEC related events and seek continuation training at every opportunity. OPSEC PM training is unit-funded.
c. Requests for OPSEC training in formal courses must be submitted per individual Service guidelines. Requests for IOSS courses may be sent directly to the IOSS (www.ioss.gov). All OPSEC PMs will advise their respective Higher Headquarters (HHQ) when training has been completed.

3.3.4 Coordination/ Relationship to other Security Programs. OPSEC must be closely coordinated with other security disciplines (see Table 3-1) as applicable. The primary focus of OPSEC analysis is to deny exploitation of open source information and observable activities.

TABLE 3-1. RELATED SECURITY DISCIPLINES AND SOURCE DOCUMENTATION

Discipline	Source Documentation
Anti-Terrorism/Force Protection Program	AFI 10-245/AR 525-13/SECNAVINST 3300.2B
Communications Security User Requirements	AFI 33-211AR380-40 /OPNAVINST 2201.3
Electronic Mail (E-mail) Management and Use	AFI 33-119/AR 25-2
Emissions Security	AFI 33-203/AR 380-53
DoD Operations Security	DoD5205.02-M
Freedom of Information Act (FOIA)	DODR 5400.7/AF SUP 1999/AR 25-55 / SECNAVINST 5720.42F / SECNAV 5211.5E
Industrial Security	AFPD 31-6/AFI 31-601/AR 380-49 / OPNAV 5540.8
Information Protection	AFPD 33-2/AR 530-1 / SECNAVINST 5510.36
Information Security	AFPD 31-4/AFI 31-401/AR 380-5 /SECNAVINST 5510.36
Network and Computer Security	AFI 33-202/AR 25-2
Personnel Security	AFPD 31-5/AFI 31-501/AR 380-67 /SECNAVINST 5510.30A
Physical Security	AFPD 31-1AR 190-13 / OPNAV 5530.14C
Privacy Act Information	AFI 33-332/AR 25-55 /SECNAVINST 5211.5D
Public Affairs Policies and Procedures	AFI-35-101 Chapters 15 and 18/AR 360-5/ SECNAVINST 5720.44B
Reporting COMSEC Deviation	AFI 33-212/AR 380-40
Technology and Acquisition Systems Security Program Protection	AFPD 63-17/AR530-1
Telecommunications Monitoring and Assessment Program	AFI 33-219/AR 380-53
Web Management and Internet Use	AFI 33-129/AR25-2/ SECNAVINST 5720.47B
The Militarily Critical Technologies List (MCTL). Refer to Appendix J.	http://www.dtic.mil/mctl/MCTL.html)
	National Aeronautics and Space Administration (NASA)
Operations Security Program	DOD Directive 5205.2
Joint Information Warfare Policy	Chairman, Joint Chiefs of Staff Instruction (CJCSI) 3210.01A
Joint Operations Security	CJCSI 3213.01
Defense Acquisition Management Policies and Procedures	DOD Instruction 5000.2

3.4 OPSEC Reporting Requirements

The OPSEC program reporting requirements include two types of time-sensitive reports:

3.4.1 OPSEC Vulnerability Reports. An OPSEC vulnerability report identifies a disclosure of critical information or provides the identification of OPSEC indicators that could jeopardize ongoing or planned operations (See Appendix B). Vulnerability reports may warrant dissemination beyond the particular unit to enable damage control measures to minimize potential exploitation by adversaries and ensure implementation of OPSEC measures. This reporting is not intended to assign blame or initiate punitive action, but rather to highlight potential vulnerabilities, identify trends, and improve the OPSEC posture of an individual Service or all the military Services. OPSEC PMs and Coordinators are the focal points for ensuring Commanders are advised of local OPSEC vulnerabilities and the importance of reporting them as part of the overall Information Operations (IO) and OPSEC program. Reports will be submitted per guidance from the individual Services. The IO Threat Analysis Center OPSEC Section can make fused reports available to OPSEC Program Managers (PM) and other entities as necessary. Vulnerability Program Reports can be submitted by Program Managers, Telephone Monitoring and Assessment Program (TMAP) teams, Multi-Disciplinary Vulnerability Assessment (MDVA) teams, Survey Teams, or the Web Risk Assessment units that identify a possible disclosure of critical information or an OPSEC indicator that jeopardizes the organization's operations. Any other individual or organization that identifies a possible vulnerability should forward through their chain of command to those entities authorized to validate and submit vulnerability reports.

MDVAs are performed to assess an installation's application of IO and security processes. MDVAs simulate various IO threats to identify an installation or organization's vulnerabilities (OPSEC, network, physical security, etc.), operational impacts if those vulnerabilities are exploited, and exercise response procedures to the simulated threat. MDVAs are not synonymous with the Joint Staff Integrated Vulnerability Assessments (JSIVA) or the Agency Vulnerability Assessment (AVA). MDVA results are detailed in a formal report to the requesting Director or Commander. An MDVA should not be used to initiate an OPSEC program or be used to prepare for an inspection. Commanders can request a MDVA by contacting their higher headquarters.

3.4.2 OPSEC Advisory Reports. An OPSEC Advisory Report provides advance notification of a potential threat to operations. Examples include flight paths of foreign aircraft over United States (U.S.) territory, location of foreign naval vessels with collection capabilities, and projected commercial satellite exploitation. Various organizations receiving these reports/notifications should maintain continuous liaison/coordination with Service specific/directed and other appropriate organizations and sources to ensure identification and timely notifications of potential threats. OPSEC PMs must review OPSEC Advisory Reports and ensure Commanders and subordinate organizations are kept informed. An example of an OPSEC Advisory Report is at Figure 3-1.

OPSEC Advisory (050502) and Recommendation:

UNCLASSIFIED//FOR OFFICIAL USE ONLY.
MSGID/GENADMIN/CDRUSSTRATCOM//
SUBJ/OPERATIONS SECURITY (OPSEC)//
GENTEXT/REMARKS/
REF/A/ DSD/MEMO/06 JUN 03/
REF/B/SD/INFORMATION OPERATIONS ROADMAP/30 OCT 03/ NARR/ REF A IS THE DEPUTY SECRETARY OF DEFENSE (DEPSECDEF) MEMORANDUM REGARDING DEPARTMENT OF DEFENSE (DOD) OPSEC.

REF B IS SECRETARY OF DEFENSE **INFORMATION OPERATIONS ROADMAP**.
1. (U//FOUO) THE SECDEF'S INFORMATION OPERATIONS ROADMAP RECOMMENDATION NUMBER 55, INSTRUCTS OSD, STRATCOM AND THE JCS TO PROMOTE COMMAND EMPHASIS ON OPERATIONS SECURITY BY KEEPING OPSEC PROCESSES VISIBLE AND BY PREPARING AND DISSEMINATING PERIODIC REMINDERS FROM DOD LEADERSHIP. AS WE PREPARE FOR THIS YEAR'S CHALLENGES, LET ME RE-EMPHASIZE THE IMPORTANCE OF OPSEC AS A FORCE PROTECTOR.

2. (U//FOUO) OPSEC REMAINS PIVOTAL TO ENABLING EFFORTS TO DETER AGGRESSION, SUSTAIN OPERATIONAL READINESS, AND PROSECUTE THE GLOBAL WAR ON TERRORISM. ALL PERSONNEL MUST UNDERSTAND AND APPLY THE PRINCIPLES OF OPSEC; EACH INDIVIDUAL HAS AN INHERENT RESPONSIBILITY TO TAKE A HARD LOOK AT INFORMATION POSTED ON UNCLASSIFIED OFFICIAL WEBSITES AND ADOPT GOOD OPSEC PRACTICES.

3. (U//FOUO) OUR ADVERSARIES EXPLOIT THE INTERNET ON A REGULAR BASIS.
A. (U//FOUO) VARIOUS INTERNET WEB SITES CAN BE USED AS GOOD SOURCES OF INFORMATION ABOUT DOD PLANS, PROGRAMS AND OPERATIONS. FOR EXAMPLE, CRITICAL INFORMATION PUBLISHED ON COMMERCIAL OR PRIVATE WEB SITES AND NEWS GROUPS CONCERNING TRANSIT AND ARRIVAL TIMES FOR US MILITARY UNITS COULD BE USED TO FACILITATE AN ATTACK.

B. (U//FOUO) NIPRNET EMAILS AND ATTACHMENTS ARE ALSO VULNERABLE TO EXPLOITATION. EMAILS CONTAINING RECALL ROSTERS, KEY PERSONNEL LISTS, ITINERARIES, TACTICS, TECHNIQUES AND PROCEDURES, AND LESSONS LEARNED PAPERS REVEAL INFORMATION THAT PUTS OUR TROOPS AND POSSIBLY EVEN FAMILIES AT RISK. INFORMATION NOT TRANSMITTED OVER SECURE OR CONTROLLED CHANNELS IS SUBJECT TO COMPROMISE.

4. (U//FOUO) IN VIEW OF THE FACTS, WE SHOULD CONTINUALLY STRESS THREE SIMPLE, BUT IMPORTANT, COUNTERMEASURES TO REDUCE OTHER VULNERABILITIES:

> **A. (U//FOUO) SECURE COMMUNICATIONS. USE STUS/STES FOR VOICE COMMUNICATIONS WHEN DISCUSSING MILITARY OPERATIONS.**
>
> **B. (U//FOUO) SIPRNET. USE THE SIPRNET INSTEAD OF THE NIPRNET FOR RECORD COMMUNICATIONS. CONTINUALLY REVIEW AND KEEP SENSITIVE INFORMATION OUT OF THE PUBLIC DOMAIN.**
>
> **C. (U//FOUO) SHRED. BURN OR SHRED ALL OFFICE DOCUMENTS WHEN NO LONGER NEEDED.**

CHARLES P. SIPES, GG-13, DAF
HQ AIA OPSEC Program Manager
HQ AIA/DOOI

Classification: UNCLASSIFIED//FOR OFFICIAL USE ONLY

Figure 3-1. OPSEC Advisory Report (an example).

CHAPTER 4

THE OPSEC SURVEY

4.1 OPSEC Survey (Overview)

The OPSEC survey is a systematic process to examine the actual practices and procedures employed by an activity or operation to achieve its goals. The methodology consists of using a team of experts to look at an activity through the eyes of an adversary to determine if critical information may be inadvertently disclosed through the performance of normal organizational functions. The primary purpose is to evaluate and improve organizational effectiveness and to control the vulnerabilities of friendly actions or information.

The survey will determine if the critical information identified during the OPSEC planning process is being protected or controlled. A survey cannot be conducted until after an organization has at least identified its critical information. Without a basis of identified critical information, there can be no specific determination that actual OPSEC vulnerabilities exist.

4.2 Uniqueness

4.2.1 Nature of Surveys. Each OPSEC survey is unique. Surveys differ in the nature of the information requiring protection or control, the adversary collection capability, and the environment of the activity to be surveyed.

4.2.2 Emphasis. In times of crisis or conflict, a survey's emphasis must be on identifying operational indicators that signal friendly intentions, capabilities and/or limitations and that will permit the adversary to counter friendly operations or reduce their effectiveness.

4.2.3 Peacetime Surveys. In peacetime, surveys generally seek to correct weaknesses that disclose information useful to potential adversaries. Many activities, such as mobility exercises, cradle-to-grave acquisition processes, and day-to-day operations/training are of strategic interest to potential adversaries as they provide insight into friendly readiness, plans, and capabilities.

4.3 OPSEC Surveys versus Security Inspections

4.3.1 Definitions. The OPSEC surveys are different from security evaluations or inspections. A survey attempts to produce an adversary's view of the operation or activity being surveyed. A security inspection seeks to determine if an organization is in compliance with the appropriate security directives and regulations.

4.3.2 Planned versus Random. Surveys are planned, coordinated, or conducted by the organization responsible for the operation or activity that is to be surveyed. Inspections may be conducted without warning by outside organizations.

4.3.3 Assessments. OPSEC surveys are not a check on the effectiveness of an organization's security programs or its adherence to security directives. Instead, survey teams will assess how current security measures positively or negatively affect OPSEC.

4.3.4 Non-Punitive Objective. Surveys are not punitive by nature and no grades or evaluations are awarded because of them. Surveys are not designed to inspect individuals but to evaluate practices and procedures used to accomplish the mission. Unless this non-punitive objective is made clear, team members will inevitably appear as inspectors, which may hamper cooperation and assistance from the surveyed organizations.

4.4 Types of Surveys

The two basic types of OPSEC surveys are "formal" and "command (in-house)." Both types follow the same basic sequence and procedures that are established in this attachment.

4.4.1 Formal Survey. A formal survey concentrates on activities that cross organizational lines. It requires a survey team composed of members from inside and outside the command.

4.4.2 Command (In-house) Survey. A command survey concentrates on activities within the particular command/unit. It is performed using only command/unit (in-house) personnel. This is the most common survey for Air Force units.

4.5 Survey Execution.

Careful prior planning, thorough data collection, and thoughtful analysis of the results are the key phases of an effective survey. The three phases to an OPSEC survey are:

a. Planning Phase — Paragraph 4.5.1
b. Field Survey Phase — Paragraph 4.5.2
c. Analysis and Reporting Phase — Paragraph 4.5.3

4.5.1 OPSEC Survey Planning Phase. Preparations for an OPSEC survey must begin well in advance of the field survey phase. The required lead-time will depend on the nature and complexity of the operation and activities to be surveyed (contingency operation, peacetime operational activity, or other type of operation). Sufficient time must be allotted in the planning phase for a thorough review of pertinent documentation, for formal and informal coordination and discussions, and for the careful preparation of functional outlines. The appropriate unit actions normally make up the planning phase.

a. Determine the Scope of the Survey. The scope of the survey should be defined at the start of the planning phase and be limited to manageable proportions. For example, an internal command survey conducted by a squadron would require less time and coordination than a formal survey and would be limited to actions within the resource and manpower limitations of the squadron. Geography, time, units to be observed, funding, and other practical matters will also impose limitations.

b. Select Team Members. Regardless of the survey's focus, the team should contain multidiscipline expertise. Survey team members should be selected for their analytical, observational, and problem-solving abilities.
   (1) Since surveys are normally oriented to operations, the senior member should be selected from the operations (or equivalent) staff of the Commander responsible or conducting the survey. Typical team members would represent the functional areas of intelligence, security, counterintelligence, communications, logistics, plans, and personnel. When appropriate, specialists from other functional areas, such as transportation and public affairs, will participate.
   (2) When TMAP is planned as part of the survey, the monitoring team's mission supervisor or senior analyst should be designated as a member of the OPSEC survey team. Team members must be brought together early in the planning phase to ensure timely, thorough accomplishment of the tasks outlined below.

c. Become Familiar with Survey Procedures. When possible, designate team members with survey experience. Otherwise, train team members on survey procedures.

d. Determine the Adversary Intelligence Threat. The adversary threat to the organization to be surveyed must be evaluated accurately, carefully and realistically. An all-source threat assessment should comprehensively address the adversary intelligence capability, taking into account not only the adversary's collection capabilities but also the adversary's ability to exploit the collection results in a timely manner. Survey team members can obtain adversary threat information from multiple sources including the local investigative or military intelligence detachment, Defense Intelligence Agency, or other military Service intelligence agencies.

e. Understand the (Target) Organization. A thorough understanding of the organization to be surveyed is crucial to ensuring the success of subsequent phases of the survey. Team members should become familiar with the mission statement/description, OPLANs, OPORDs, CONOPs, standard operating procedures, or other directives bearing on the surveyed organization.

f. Develop a Functional Outline. A basic OPSEC survey technique involves the construction of a chronology of events that are expected to occur in the surveyed operation or activity. Events are assembled sequentially, thus creating a timeline that describes in detail the activities or plans of an operation or activity. Chronologies should first be constructed for each separate functional area, such as operations, communications, logistics, or personnel. This functional approach aids the team members in defining their separate areas of inquiry during the field or data collection phase of the survey. Later, the functional outlines can be correlated with each other to build an integrated chronology of the entire operation or activity.
   (1) During the initial review of operation plans, orders and procedures, individual team members can begin to develop functionally oriented outlines for their areas of interest. Initially, the outlines will be skeletal projections, in a narrative, table, or graph format, of what is expected to occur in the chronology for a particular functional area.

(2) Such projections can serve as planning aids for the subsequent field survey phase. For example, units and facilities associated with each of the events can be identified and geographically grouped to aid in planning the travel itinerary of team members during the field survey. Collectively, the initial functional outlines provide a basis for planning the field survey phase and constitute a basis for observation and interviews.

(3) During the field survey phase, team members will acquire additional information through observation, interviews, and other data-collection techniques, enabling further development and refinement of the functional outlines.

(4) Collectively, the outlines project a time-phased picture of the events associated with the planning, preparation, execution, and conclusion of the operation or activity. The outlines also provide an analytic basis for identifying events and activities that are vulnerable to adversary exploitation.

(5) After the chronology is assembled, vulnerabilities can be identified in light of the known or projected threat.

g. Determine Preliminary Friendly Vulnerabilities. After the adversary intelligence threats are determined, a subjective evaluation can be made of the potential friendly vulnerabilities. A vulnerability (e.g. a detectable, exploitable event) may or may not carry a security classification at the time of its identification, but such preliminary vulnerabilities must be protected from disclosure by administrative or security controls.

h. Announce the Survey. After team members are selected and are familiar with the organization to be surveyed, the organization conducting the survey should inform its subordinate and supporting organizations that a survey will be conducted so that preparations can be made to support the team during the field survey phase. The appropriate unit information should be included as follows:

(1) Survey purpose and scope.
(2) List of team members and their clearances.
(3) List of required briefings and orientations.
(4) Timeframe involved.
(5) Administrative support requirements.
(6) TMAP support requirements (if needed).

4.5.2 OPSEC Field Survey Phase. As noted previously, data collection begins in the planning phase with a review of associated documentation. During the field survey phase, interviews with personnel directly involved in the operation, together with observations and document collection, are the primary means of data collection. The appropriate unit actions are normally accomplished during the field survey phase.

a. Command Briefing on Operation to be Surveyed. This briefing is presented to the OPSEC survey team by the command directing the forces or assets involved in the operation or activity being surveyed. The purpose of the briefing is to provide the survey team with an overview of the operation from the command's point of view.

Team members should use this opportunity to clarify remaining questions about the information developed in the planning phase.

b. OPSEC Survey Team In-brief. The survey team chief presents this briefing to the Commander and principal staff officers of the surveyed organization. The briefing may be either a formal presentation or an informal discussion. The objective is to inform the Commander and the staff of how the survey will be conducted. The briefing should include a summary of the hostile threat and the vulnerability assessment developed during the planning phase. Results of previous OPSEC surveys of similar activities may be summarized. The Commander should be given the opportunity to recommend specific focus areas in which the survey team can concentrate.

c. Data Collection and Functional Outline Refinement. During the field survey phase, data is collected through observation of activities, document collection, and personnel interviews. Data may also be acquired through concurrent data collection, such as TMAP. Team members must be alert to differences between what they have read, what they have assumed to be the situation, what they have been told in the command briefing, and what they observe and are told by personnel participating in the operation. Conflicting data is to be expected. While observations can verify the occurrence, sequence, and exact timing of events, much essential information must be gathered from interviews.
   (1) Functional outlines should be reviewed before and after interviews to ensure that all pertinent points are covered. Specifics on how, when and where people accomplish their tasks and how these tasks relate to the planned and observed sequence of events, are recorded in order to document activities in a logical sequence.
   (2) Team members should assure interviewees that all sources of information will be protected by a non-attribution policy.
   Interviews are best conducted by two team members.
   (3) Facts to be recorded during or soon after the interview normally include:
      - Identification and purpose of the interview.
      - Description of the positions occupied by the persons being interviewed.
      - Details of exactly what tasks the individuals perform and how, when and where they perform them with a view toward determining what information they receive, handle, or generate and what they do with it.
      - Whether the individuals' actions reflect an awareness of a hostile intelligence collection threat.

d. Functional Outline Refinement. As indicated earlier, each team member should have a basic functional outline to direct data collection efforts at the beginning of the field survey phase. The basic outline will be modified during this phase to reflect new information obtained by observation/interview and will ultimately become a profile of actual events.
   (1) Each team member should be familiar with the outlines used by the other members of the survey team and should be alert for information that might affect them. An interview in the communications area, for example, might

disclose information that would result in a change to the outline being developed for operations; or an observation in one geographic location could affect an outline being followed up in another. Also, to permit follow-up elsewhere, all outlines should try to reflect the information generated and the flow at each location where data is collected.

(2) As data is accumulated through observation and interviews, incorporation of such data into the basic functional outline changes the original list of projected events into a profile of actual events. The functional outline then becomes a chronological record of what actually was done, where, who did it, and how and why it was done. The outline should also reflect an assessment of the vulnerability of each event to the known or suspected hostile intelligence threat. Tentative observations will begin to emerge as data collection proceeds and information is reviewed and compared. The observations should be confirmed and fully documented as quickly as possible.

(3) If an observation is considered to have serious mission impact, the organization's Commander should be immediately notified in order to permit timely corrective actions. Development of observations during the field survey phase ensures access to supporting data and precludes the need to reconstruct events after the team has departed. Following this procedure, the basic observations and supporting data of the final survey report will be well developed before the end of the field survey phase. Final development and production of the survey report can then proceed immediately upon the team's return to home station.

e. Team Employment. The complexity, size, and duration of the surveyed operation or activity will determine the general employment of the survey team. Tentative locations for data collection, developed during the planning phase, provide initial indications of how and where to employ the team. It is rarely possible to accurately plan employment in detail before the field survey phase. A limited, short duration operation with few participating elements may permit concentrating the team in one or two locations. Larger and longer operations may require complete dispersal of the team, movement of the entire team from one location to another, or both, over a substantial period. The most reliable guideline for the team chief in determining how to employ the team is to reassemble it daily to assess progress, compare data, and coordinate the direction of the survey.

The duration of the field survey phase is established during the planning phase and depends on how rapidly data is collected. The proximity of data collection locations to each other, number of such locations, transportation availability, and degree of difficulty experienced in resolving conflicting data are some of the factors affecting duration of the field survey phase.

f. OPSEC Survey Team Out-brief. An out-brief should be presented to the Commander before the team departs, regardless of previous reports or tentative observations. Like the in-brief, the out-brief can be an informal discussion with the Commander or a formal briefing for the Commander and the staff. The tentative nature of survey observations should be emphasized. Even those that appear to be firm may be altered

by the final data review as the survey report is prepared. Because preparation of the written report may take some time, the out-brief can serve as an interim basis for further consideration and possible action by the Commander. The distribution of the final written report should be clearly stated during the out-brief. Normally, the report will be provided directly to the Commander. DoD Distribution statements can be seen at Appendix K.

4.5.3 Analysis and Reporting Phase. During this phase, the OPSEC team correlates the data acquired by individual members with information from any other assessments conducted in conjunction with the survey.

a. Correlation of Data.
   (1) Correlation of Functional Outlines. When the separate chronology outlines for each functional area are correlated, the chronology of events for the organization will emerge. Data from the field survey and analytic phases must not conflict with each other.
   (2) Functional Outlines. The purpose of constructing the functional outlines is to describe the time-phased unfolding of the operation or activity; to depict the manner in which separate commands, organizations and activities interact and perform their roles in the operation or activity; and to trace the flow of information from its origin to its ultimate recipients. It is important that the team members present the information in a manner that facilitates analysis. The net result of the correlation will portray the practices and procedures of the entire organization.

b. Identification of Vulnerabilities.
   (1) Correlation and Analysis. The correlation and analysis of data helps the team refine the previously identified preliminary vulnerabilities or isolate new ones. The analysis is accomplished in a similar manner that adversaries would process information through their intelligence systems.
   (2) Indicators. Potentially observable indicators are identified as vulnerabilities. The key factors of vulnerability are observable indicators and an intelligence collection threat to those indicators. The degree of risk to the friendly mission depends on the adversary's ability to exploit these vulnerabilities and react to the situation in sufficient time to degrade the organization's mission.

c. OPSEC Survey Report. The OPSEC survey report is addressed to the Commander of the surveyed organization. The report provides a discussion of identified critical information, indicators, adversaries and their intelligence capabilities, OPSEC vulnerabilities, risk analysis and recommended OPSEC measures to eliminate or reduce the vulnerabilities. Although some vulnerabilities may be virtually impossible to eliminate or reduce, they should be included in the report to enable Commanders to realistically assess their organization.
   (1) Threat Statement. Each report should contain a threat statement. Its length and classification need only be adequate to substantiate the vulnerabilities (or actual sources of adversary information) described in the report. Portions of the threat that apply to a particular observation should be substantiated in the report. If

the classification level of the threat statement impedes the desired distribution and handling, consider attaching the threat statement in a separate annex to the report. DoD Distribution statements can be seen at Appendix K.

(2) Corrective Actions. Recommendations for corrective actions should also be included in the report. However, the team is not compelled to accompany each observation with a recommendation. In some situations, the team may not be qualified to devise the corrective action; in others, it may not have an appreciation of the limitations in resources and options of a particular command. Ultimately, Commanders must assess the effect of possible adversary exploitation of vulnerabilities on the effectiveness of their operation or activity. They must then decide to implement corrective actions or accept the risk posed by the vulnerability.

(3) Appendices and Annexes. Appendices and annexes to OPSEC survey reports may be added to support the observations, conclusions, and recommendations. Some examples include threat assessments, maps, diagrams, and other illustrative materials.

(4) Conclusion/Summary. The report may end with a conclusion or summary of the survey and its findings. The summary should not include judgments about compliance with standing security practices of the organizations. Such judgments are the purview of security disciplines.

(5) Control. Because they contain vulnerability information, OPSEC survey reports must be controlled from release to unauthorized persons or agencies. Affected portions of the report must be controlled in accordance with applicable security classification guides. For those portions of the report not controlled by security classification guides, administrative control of the release of survey report information must be considered. Likewise, the notes, interviews, and raw data used to build a survey report must be subject to the same controls as the finished report.

(6) Unit Pages. The appropriate unit pages contain information and documentation to be used during the entire survey process. This information is to be used as a guide and units are to limit the scope of their survey to available manpower and resources.

4.6 OPSEC Survey Planning Worksheet

Phase 1 refers to all preparations done prior to the team beginning the information-gathering phase of the survey, which includes threat research, preparatory interviews and preliminary documentation search.

Phase 2 refers to the period when the entire team comes together, conducts interviews, holds daily team meetings, completes the analysis, and reports the results.

The completed planning worksheet (Appendix E) may be provided to team members at the beginning of Phase 2 in lieu of a written survey plan. Attachments too lengthy to provide individual copies can be made available in a separate notebook.

CHAPTER 5

ORGANIZATIONAL OPSEC PLANNING

5.1 Purpose and Composition

Unit OPSEC programs support the Commander's efforts to accomplish a successful and effective mission. Each program is composed of an OPSEC PM or Coordinator, OPSEC plans, funding, training, assessments, and feedback. Unit OPSEC programs must have the appropriate unit critical aspects: Commander involvement, operational focus, integration, coordination, and self assessment.

5.1.1 Commander Involvement. Commanders are responsible for ensuring OPSEC is integrated into day-to-day operations. Commanders may delegate authority for OPSEC program management, but retain responsibility for risk management decisions and the overall implementation of OPSEC measures.

5.1.2 Operational Focus. The OPSEC program is an operations program and its goals are information superiority and optimal mission effectiveness. The emphasis is on OPERATIONS and the assurance of effective mission accomplishment. The unit PM and Coordinator should reside in the operations or plans element of an organization or report directly to the unit Commander to ensure effective implementation across organizational and functional lines. However, for those units with no traditional operations or plans element, the Commander must decide the most logical area to place management and coordination of the unit's OPSEC program while focusing on operations and the mission of the unit.

5.1.3 Integration. PMs and coordinators will integrate OPSEC into all organizational plans and activities. Staff elements and supporting organizations will ensure OPSEC is appropriately incorporated at the earliest possible time into all Operations Plans (OPLANs), Concept Plans (CONPLANs), Concept Of Operations (CONOPs), operations orders (OPORDs), exercise plans, Initial Capability Documents (ICD), Capability Development Documents (CDD), Initial Requirement Documents (IRD), Program Protection Plans (PPP), operating procedures and other plans and activities to ensure consistent control of critical information and OPSEC indicators. All applicable contracts, Statements of Work (SOW), Requests for Proposals (RFP) and similar documentation will contain specific statements or requirements that address security criteria for protecting critical information and OPSEC indicators. All OPSEC PM.s and coordinators will ensure OPSEC is incorporated in all organizational plans. All OPSEC PMs and coordinators will add an OPSEC section to each respective annex to all organizational plans. The appropriate functional area OPSEC PM or coordinator will evaluate all appropriate contractual documents regarding OPSEC and will work with the local contracting office to ensure the intent of the program is met.

a. The OPSEC must be an integral part of an overall Information Operation (IO) effort. This applies to other IO and Influence Operations functions that also protect friendly information and that may influence the adversary's decision-making process. The public affairs office OPSEC Coordinator will ensure the public affairs office members are aware of critical information. For example, integration of OPSEC and

Public Affairs is particularly important as the need to protect critical information must be balanced against the desire to provide information to the public. The PM or coordinator will maintain copies of all applicable Public Affairs guidance and ensure the Public Affairs office is aware of critical information elements.

b. The OPSEC is integrated into the Area of Concern (AOC) through the IO Team. The IO Team OPSEC coordinators/planners work within the AOC to ensure planning and execution of air, space and IO incorporate OPSEC. IO Team OPSEC coordinators/planners work with the rest of the IO Team to integrate OPSEC with other IO activities. When an AOC is formed, IO Team OPSEC coordinators/planners become the focal point for integrating the activities of supporting commands OPSEC PMs and coordinators. This ensures the applicable Service Commander has a coherent OPSEC effort across all Service units.

5.1.4 Coordination. OPSEC must be coordinated with IO. Coordination across functional and organizational lines facilitates OPSEC planning and enhances the effectiveness of OPSEC measures.

5.1.5 Self Assessment. Self assessments should be performed at least annually using the agency or unit approved self assessment tool. A sample of a self assessment checklist is provided at Appendix D.

5.2 OPSEC Plan

Each unit will have a written OPSEC Plan. Recommended contents for an OPSEC Plan can be seen at Appendix L. However, OPSEC PMs and coordinators will use their applicable Service's guidelines, when developing these plans since this tactics, techniques and procedures (TTP) provides the "how to" for planning and executing IO and OPSEC. All OPSEC plans will utilize the plan format listed in Service specific guidelines:

5.3 OPSEC Document Reviews

Each document generated for official processes or activities must be evaluated for operationally sensitive information known as essential elements of friendly information, critical indicators, critical program indicators, or operationally critical information. This information is typically tabulated in a document known as a Critical Information List and is defined in various agency guidance such as AFI 10-701. Each document author is responsible for reviewing the document they publish for technical accuracy (Subject Matter Expert review) and operations security review (critical information review). This process is provided at Appendix O. The form required to be submitted with each document publication request to the RCC Secretariat is described in Appendix P.

REFERENCES

a. National Security Decision Directive (NSDD) No. 298, National Operations Security Program.

b. Joint Publication (JP) 3-54, Joint Doctrine for Operations Security.

c. Air Force Instruction (AFI) 33-129 (AFI 33-129), Web Management and Internet Use

d. Air Force Instruction (AFI) 33-219, Telecommunications Monitoring and Assessment Program (TMAP).

e. DoD Instruction (DoDI) 2000.16 Red Teaming Requirement.

f. Air Force Instruction (AFI) 10-701, Operations Security (OPSEC) http://www.dtic.mil/mctl/MCTL.html), The Militarily Critical Technologies List (MCTL).

g. DoD Directive (DODD) 5205.2, DoD Operations Security (OPSEC) Program.

h. DoD Directive (DODD) 5100.20, The National Security Agency and the Central Security Service

i. DoD Directive (DODD) 5200.39, Security, Intelligence, and Counterintelligence Support to Acquisition Program Protection.

j. CJCSI 3213.01B, Joint Operations Security.

k. DoD Directive (DODD) 3600.1, Information Operations.

l. DOD 5230.9, Clearance of DoD Information for Public Release.

m. DoD Directive (DODD) 8500.1, Information Assurance.

n. DoD Instruction (DODI) 5000.2, Operation of the Defense Acquisition System.

o. DoD Directive (DODD) 5200.1-R, DoD Information Security Program.

p. DoD Directive (DODD) 5200.39, Security, Intelligence, and Counterintelligence Support to Acquisition Program Protection.

q. DoD Directive (DODD) 5205.2, *DoD Operations Security (OPSEC) Program.*

r. Air Force Doctrine Document (AFDD) 2-5, Information Operations.

s. Air Force Policy Directive (AFPD) 10-7, Information Warfare.

t. Air Force Policy Directive (AFPD) 90-2, Inspector General -- The Inspection System.

This page intentionally left blank.

APPENDIX A

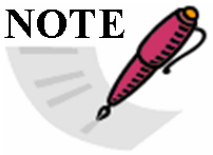
RESPONSIBILITIES AND AUTHORITIES

1.1 Commanders of the Range Commanders Council (RCC)

The Commanders, RCC will:

a. Assign OPSEC tasks to the Chairperson, Range Operations Group (ROG) for completion by the ROG.
b. Approve common OPSEC measures developed by the ROG to be applied to the members of the RCC.

1.2 Range Operations Group (ROG)



There is no formal/standing OPSEC Committee as of the publication date. Therefore, the use of the term "OPSEC Committee" herein refers to any committee created by the ROG for accomplishment of a specific OPSEC assignment assigned by the Commanders.

The Chairperson of the ROG will:

a. Assign OPSEC tasks assigned to the ROG to an OPSEC Committee for completion.
b. Monitor progress on each task assigned to the Range OPSEC Committee and report progress to the Secretariat of the RCC.
c. Within their capabilities, provide technical guidance and assistance to the OPSEC Committee to ensure that member ranges provide support to the assigned lead for each assigned task.
d. Encourage each member range to participate in the Range OPSEC Committee and to provide a representative to support the committee.
e. Interpret OPSEC policies of senior authorities and recommends organizational policies. Facilitate the implementation of OPSEC throughout their organization to include OPSEC measures that are determined to the common to the test ranges and that they conform to guidance from higher authorities and or specific operation/system program manager’s guidance.
f. Integrate OPSEC into organizational plans and activities, Information Operations/Information Warfare (IO/IW), force protection strategies and required/critical plans for test/operations/training support to customers as required.
g. Advise Commanders and other decision makers on OPSEC matters.
h. Coordinate (and facilitate the development of) OPSEC plans and measures for operations, activities, and exercises.
i. Coordinate with other security functions that complement OPSEC.
j. Ensure critical information is identified and controlled.
k. Assist in determining operational requirements for security and guidelines for the release of information.

l. Determine guidelines for controlling critical information and sensitive activities.
m. Coordinate and facilitate OPSEC surveys as required.
n. Forward recommendations for policy change or program modification to through appropriate channels.
o. Serve as focal point for OPSEC event reporting.

APPENDIX B

DOCUMENTING VULNERABILITIES AND INDICATORS

Some vulnerabilities and indicators will be common among the test ranges and facilities; these will be identified by the supporting investigative or military intelligence unit. Since vulnerabilities are classified, vulnerabilities will be identified and documented by each organization for their specific mission.

a. OPSEC vulnerability existence. An OPSEC vulnerability exists when the adversary is capable of collecting an OPSEC indicator, analyzing it, and then acting quickly enough to affect their decision-making process. Vulnerabilities are weaknesses that reveal critical information through collected and analyzed indicators.

b. OPSEC indicators. OPSEC indicators are those friendly actions and information that adversary intelligence efforts can potentially detect or obtain and then interpret to derive friendly critical information. Indicators may be classified or unclassified.

This page intentionally left blank.

APPENDIX C

DOCUMENTED MEASURES AND COUNTERMEASURES

1.1 Commonality of Measures/Countermeasures

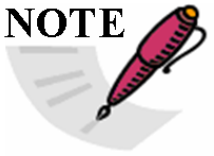
Some security measures/countermeasures will be common among the ranges and facilities. These will be identified by the supporting investigative or military intelligence unit. Since these measures are classified, they will be documented by each organization for their mission.

Recommended OPSEC measures are designed to preserve military capabilities by preventing adversarial exploitation of critical information. OPSEC measures are employed to mitigate or exploit vulnerabilities that point to, or divulge, critical information. They help control critical information by managing the raw data and enhance friendly capabilities by increasing the potential for surprise and effectiveness of friendly military forces and weapons systems.

1.2 Categories of OPSEC Measures

OPSEC measures consist of a combination of Information Operations (IO) capabilities to counter an adversary's ability to gain and exploit friendly information. These measures must be implemented as part of an overall IO effort to influence an adversary's perceptions and situational awareness. OPSEC measures fall under three general categories:

a. Preventing the adversary from detecting critical information and indicators. The objective is to eliminate or disrupt effective adversary information gathering of indicators or the vulnerability of actions to exploitation by adversary intelligence systems.
b. Providing alternative deceptive interpretations of critical information and/or indicators. Sometimes it may not be cost-effective to control actions that reveal critical information or become the source of an OPSEC indicator. In these circumstances, measures attempt to influence and affect the adversary's ability to properly interpret the information.
c. Attacking the adversary's collection system. This means using IO capabilities or kinetic operations to attack an adversary's intelligence collection system to eliminate or reduce their ability to obtain critical information. Two examples are an electronic attack against technical collection platforms and the physical destruction of intelligence fusion and analysis centers.

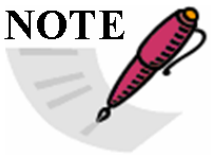


All OPSEC measures should be synchronized with other components of IO and implemented as part of an overall IO effort to influence the adversary's perceptions and situational awareness. Care must be taken so that OPSEC measures do not become unacceptable indicators themselves.

This page intentionally left blank.

APPENDIX D

SELF ASSESSMENTS: OPSEC INSPECTION CHECKLIST (EXAMPLE)



This is an example based on Air Force Instruction (AFI) 10-701 (see Reference f). You should use the appropriate Service-specific checklist. This example can be used to develop your own inspection checklists based on the reader's particular organizational level and/or OPSEC requirements in accordance with guidance contained in this document.

1.1 Administrative Requirements

1.1.1 Commander or Director (all levels). Has the Commander or Director::

a. Appointed an OPSEC Program Manager (PM) or coordinator and PM Alternate in writing?
b. Ensured the OPSEC PM or coordinator has a security clearance appropriate to the mission and function of the organization, but not lower than Secret?

1.1.2 OPSEC PM and/or Coordinator.

a. Does the appointee reside in the operations or plans element of the organization or report directly to the organization's Commander?
b. Has his/her identity been forwarded to the higher headquarters (HHQ) OPSEC PM?
c. Is the OPSEC PM/coordinator aware of their responsibilities?

1.2 OPSEC Execution Requirements

1.2.1 Has the Commander:

a. Developed an OPSEC program in accordance with DoD Service policy and guidance?
b. Ensured their organization has integrated OPSEC within day-to-day operations?
c. Made OPSEC risk management decisions?
d. Directed the overall implementation of OPSEC measures?
e. Ensured OPSEC is integrated with other IO activities and efforts?

1.2.2 Has the OPSEC PM:

a. Developed, coordinated, and managed the OPSEC program?
b. Overseen development of Commander's policy and creation of CILs)?
c. Developed procedures to ensure subordinate units are controlling critical information and indicators?
d. Ensured subordinate units plan, exercise, and implement OPSEC measures as appropriate?

e. Developed, coordinated, and implemented an OPSEC plan?
f. Incorporated OPSEC into organizational plans, exercises, activities, and command-to-command agreements?
g. Incorporated OPSEC lessons learned from unit operations and exercises as well as other operations and exercises into the planning process and forward lessons learned to appropriate depositories?
h. Ensured all applicable contracts, Statements of Work (SOW), Requests for Proposals (RFPs) and similar documentation contained specific statements or requirements that address security criteria to protect OPSEC-critical information and indicators?
i. Ensured OPSEC considerations are integrated into the acquisition cycle?
j. Developed and cultivated the intelligence and counterintelligence relationships necessary to support their OPSEC program?
k. Ensured OPSEC considerations are included in annual unclassified web page reviews and in the approval process for posting new data to the web?
l. Ensured OPSEC considerations are included in PA's review and approval process for the publishing and/or releasing of information to or that may be viewed by the public?
m. Coordinated and facilitated OPSEC assessments?
n. Completed an annual self-assessment of their program and each subordinate organization?
o. Coordinated their OPSEC program with host or tenant unit OPSEC Managers and/or Coordinators?
p. Ensured OPSEC is integrated with other Information Operations (IO) activities and efforts?
q. Formed and chaired the OPSEC Working Group consisting of appropriate IO and security disciplines and applicable supporting organizations?
r. Conducted Staff Assistance Visits (SAVs) to all subordinate units as required?
s. Ensured all subordinate units are controlling critical information and indicators as required?
t. Ensured all subordinate units plans, exercises, and implemented OPSEC measures as appropriate?
u. Ensured OPSEC considerations are included in Initial Capabilities Documents, Capability Development Documents and inputs to the combatant Commanders' Integrated Priority Lists as appropriate?
v. Ensured OPSEC reviews consider the proliferation of internet/web-based bulletin boards and logs (Blogs)?
w. Serve as the focal point for TMAP?
x. Established and chaired an appropriate unit-level OPSEC working group (OWG)?
y. Requested (for the Commander or Director) an MDVA as required.

1.2.3 Has the OPSEC Coordinator:

a. Implemented and executed OPSEC utilizing Commander and OPSEC PM policy and guidance?
b. Incorporated OPSEC into organizational plans, exercises, and activities?
c. Submitted lessons learned from operations and exercises to respective HQ OPSEC PM?
d. Overseen development and implementation of Commander's OPSEC policy and CIL?
e. Developed procedures to ensure critical information is controlled and indicators identified?
f. Conducted OPSEC reviews on unit web pages prior to information being placed on the web page?
g. Ensured OPSEC reviews are conducted on information to be published or released to or that may be viewed by the public?
h. Conducted an annual OPSEC survey?
i. Participated in OPSEC Working Groups as required?
j. Coordinated and forwarded OPSEC assessment requirements to HHQ, in accordance with Chapter 5, AFI 10-701?
k. Utilized assessment results to correct discovered vulnerabilities and aid organization OPSEC awareness efforts?
l. Integrated OPSEC into all acquisition programs and contractor support documents? i.e., SOW, RFP and similar documentation will contain specific statements or requirements that address security criteria for protecting OPSEC critical information and OPSEC indicators.
m. Coordinated their OPSEC program (tenant units only) with host unit OPSEC PMs and/or Coordinators?
n. Coordinated with appropriate organizations and appropriate unit equivalent senior leadership to resolve/mitigate Web Risk Assessment, TMAP, MDVA, and other OPSEC assessment findings as required?
o. Serve as the unit focal point for TMAP

1.3 Training Requirements

1.3.1 Has the OPSEC PM:

a. Attended OPSEC PM training within 90 days of their appointment or are scheduled for the next available OPSEC PM course?
b. Ensured OPSEC training for coordinators below appropriate unit level is scheduled within 90 days of appointment, or by the next available class?
c. Ensured all OPSEC Planners and personnel performing OPSEC surveys and IG inspections are provided OPSEC training?
d. Maintained a general awareness of current OPSEC related events and sought continuation training at every opportunity?
e. Ensured mission-oriented OPSEC education and awareness training was provided to all personnel on an annual basis?

1.3.2 Has the OPSEC coordinator (below appropriate unit-level):

a. Been scheduled for OPSEC training within 90 days of the assignment as an OPSEC Coordinator?
b. Provided management and oversight of initial OPSEC training upon arrival of newly assigned personnel (military, civilian, and contractors) and recurring training annually thereafter?
c. Ensured OPSEC training for newcomers and annual recurring training contain, as a minimum the unit's critical information, threats to the unit and applicable OPSEC measures to be used?
d. Tracked and documented training for all military, civilian and contractor personnel?

1.4 OPSEC Assessment Requirements

1.4.1 Has the OPSEC PM (command-level) coordinated closely with subordinate organization to determine assessment requirements?

1.4.2 Has the OPSEC PM (unit/appropriate unit-level) conducted annual SAVs of their subordinate units as requested or required?

1.4.3 Has the OPSEC PM or Coordinator:

a. Conducted an annual self-assessment?
b. Had a telecommunications monitor conducted as part of a survey, an MDVA, or a stand-alone assessment at least biennially?
c. Conducted or had an outside agency conduct a survey?
d. Ensured OPSEC reviews considered the proliferation of internet/web-based bulletin boards and logs (Blogs) and evaluate the risk presented by web content in annual OPSEC assessments?

1.5 OPSEC Reporting Requirements

1.5.1 Has the OPSEC PM:

a. Developed and submitted to HHQ an annual budget requirement for inclusion into command and HQ USAF POM process?
b. Forwarded their self-assessment findings containing If an OPSEC vulnerability is discovered and cannot be resolved locally or has potential to affect other outside units the OPSEC PM can request HHQ assistance.:
   (1) Training metrics for all subordinate units?
   (2) Number of vulnerability reports forwarded to the IO Threat Analysis Center?
   (3) Number and type of survey/assessment received by subordinate units (command survey, TMAP, MDVA, Web Risk Assessments, etc.)?
   (4) Any other information deemed of OPSEC importance to their HHQ OPSEC PM NLT 30 September and of each year?

c. Ensured OPSEC vulnerability reports are forwarded to HQ AIA's IO Threat Analysis Center or equivalent in a timely manner?

1.5.2 Has the OPSEC Coordinator:

a. Forwarded their self-assessment findings containing:
   (1) Training metrics for all personnel
   (2) Number of vulnerability reports forwarded to the IO Threat Analysis Center or equivalent,
   (3) Number and type of survey/assessment conducted (command survey, TMAP, MDVA, Web Risk Assessments, etc.),
   (4) Any other information deemed of OPSEC importance to their HHQ OPSEC PM NLT 15 September of each year?
b. Submitted OPSEC vulnerability reports for forwarding to HHQ or AIAs IO Threat Analysis Center or equivalent in a timely manner?

This page intentionally left blank.

APPENDIX E

OPSEC SURVEY PLANNING WORKSHEET

Note: Instructions are provided at the end of this worksheet.

1	Team Leader Name		
2	Program, activity or unit to be surveyed		
3	Dates:		
4	Team expertise required	o OPSEC o Counterintelligence (CI) o Physical Security o Intelligence o Other: o Other: o Other:	o Computer Security o Systems Management o Communications o Local Mission o Other: o Other: o Other:
5	Request team members from internal sources Due:	o Operations _____ o Communications _____ o Logistics _____ o Intelligence _____ o Security _____ o Security _____ o Security _____ o Security _____ o Admin _____ o Other _____ o Other _____ o Other _____ o Other _____ o Other _____ o Other _____ o Other _____	

6	Request team members from external sources Due:	o IOSS o AFIWC o Other:	o CI (AFOSI, NCIS, Army MI) o TMAP monitoring o Other:
7	Team member clearances POC: Due:	Send clearances to: o Clearances received	
8	Augmentee/instructor funding POC: Due:		
9	Billeting required for any team members? o Yes o No POC: Due:	Name: Dates: Location:	
		Name: Dates: Location:	
		Name: Dates: Location:	
		Name: Dates: Location:	
		Name: Dates: Location:	
		Name: Dates: Location:	
		Name: Dates: Location:	

10	Open Source Research Provide a summary of information found in open source as attachment 1. POC: Due:	Data Bases
		Key Words
11	Threat Report Request a threat analysis report and provide as attachment 2. POC: Due:	Address to:
		Address to:
		Address to:
		Specific information to request:

12	Local documents POC: Due:	o Phone books o Welcome packets o Circulars o Critical Information list		o Operating Instructions o Local newspaper o Local newsletter(s) o Other
13	Arrange working space for the team POC: Due:	Location: _____ Hours available: _____		
14	Arrange administrative support for the team POC: Due:	Name/Phone/Email:		
15	Schedule in brief POC: Due:	Date:	Time:	Location:
16	Schedule threat brief POC: Due:	Date:	Time:	Location:
17	Schedule mission brief POC: Due:	Date:	Time:	Location:
18	Schedule dry run out brief POC: Due:	Date:	Time:	Location:
19	Schedule out brief POC: Due:	Date:	Time:	Location:

20	Pre-survey interviews List team member responsible for each interview; team members should provide a summary of their interview to the team leader. Attach these summaries as attachment 3. Interview summaries are due:	o Commander or Director	
		o Survey activity Director	
		o Communications manager	
		o Network manager	
		o Computer Security officer	
		o COMSEC officer	
		o Security manager	
		o Physical security support	
		o Other:	
		o Other:	
		o Other:	
		o Other:	
		o Other:	
21	Initial interview list POC: Due:	Include a list of personnel who should be interviewed when Phase 2 starts as attachment 4; include contact information for each person.	
22	Team member list POC: Due:	The team leader should compile a complete list of team members with contact information. If possible, identify partners. You may want to match interview teams with functional areas, at least to get started. Include the list as attachment 5.	
23	Commander's Letter POC: Due:	During Phase 2, every team member should carry a letter from the Commander (or designee) identifying the team members and their authority to conduct interviews. This letter, along with appropriate picture identification, should admit team members to work areas and provide adequate identification for interviews.	
24	Adversary Strategy POC: Due:	Prepare a preliminary adversary strategy based on the team leader's assessment of adversaries to be included in the survey analysis. See sample adversary strategy template below.	
25	Process Diagram POC: Due:	Prepare a preliminary process diagram for the primary survey topic based on pre-survey interviews above.	

26	(NOTES PAGES)	

INSTRUCTIONS: OPSEC SURVEY PLANNING WORKSHEET

(The team leader has oversight responsibility for the completion of this worksheet, but should enlist members of the team to be responsible for specific action items and assign a due date for each action.)

Item 1. Self-explanatory.

Item 2. Enter the name of the project, activity, or unit to be surveyed, such as "Operation Fire Fly;" or assign a designator to the survey, such as "61TAG–1" (organization name) (first survey) or "61TAG–0101" (organization name) (fiscal year) (first survey).

Item 3. Enter the dates of Phase 2.

Item 4. Identify those expertise areas you will need represented on your team, based on the Commander's requirements and the subject to be surveyed. If you anticipate needing access to such expertise to answer questions, but do not anticipate needing that expertise from team members, then make a notation of your need.

Item 5. Identify the names of individuals within your own organization you would like to have on the team and their assigned functional areas.

Item 6. Identify which organizations you will need to ask for augmentees.

Item 7. All team members including those from outside units will need to provide proof of a current security clearance. Indicate the address, the date those clearances need to be confirmed and check the box when this action is complete.

Item 8. If you are asking for help from organizations other than your own, provide financial assistance for augmentee or instructor travel. This space is for whatever notes you need to complete this action.

Item 9. Team members may need assistance with billeting depending on the travel requirements for the OPSEC survey to be conducted. Be sure this is discussed and addressed as part of the planning phase.

Item 10. You will need to do some open source research to prepare for your survey. List the databases and key words you want to use.

Item 11. You should request a written threat report, which will become part of your final report. You may want to request threat information from more than one source; the checklist allows room for three. Also indicate any specific information you have requested.

Item 12. Indicate which local documents you want to have on hand for the team.

Item 13. The team will need a work area where you can hold team meetings in private, where team members can sit to write up interviews and their observations for the report. A white board or flip chart and a bulletin board in the room are very helpful.

Item 14. Administrative support for the team can be very helpful. This individual may not be needed until the last three days prior to the out-brief, but someone who has access to the local networks and is a proficient typist can relieve some of the administrative burden from the team. Someone who is good with briefing preparation may also be useful.

Item 15. Schedule a formal in-brief with the Commander or program Director and anyone else he/she feels appropriate. The purpose of the in-brief is to introduce the team, outline your task, and get any last minute instructions from the Commander.

Item 16. Schedule a formal threat brief for the team (if this wasn't done earlier in planning). If this action is not required, just indicate "N/A."

Item 17. Schedule an organizational mission brief for the survey team. Most organizations have a standard briefing that outlines the mission; that's what you want to hear, even if you think you already know all the information. This is especially important when you have augmentees on your team. If nothing else, it allows the team to see what the organization is briefing to outsiders.

Item 18. Schedule a dry run out-brief for the afternoon of the day before your formal out-brief. All team members should have the date, time and location prior to starting interviews and should invite everyone interviewed to the dry run. All team members should attend and you should encourage attendance of those with responsibility for areas you will be including in your report. For instance, if you're briefing insufficient secure communications, be sure those responsible for providing those communications are at the dry run. The dry run has two purposes. First, it gives the team leader a chance to go through the out-brief once with all team members present to provide clarification on rough spots. Second, it gives you a chance to enlist the aid of those responsible for the areas where the team found problems rather than causing any hard feelings or alienation and gives you one last validation of what you will report.

Item 19. Schedule a formal out-brief with the Commander or his representative. It is a good idea to encourage the Commander to have all functional area managers attend. The purpose of the out-brief is to tell the leadership what your survey found and to set the tone for follow-up actions on the part of the organization. In the best situation, the Commander will assign actions and suspense dates for every observation during the briefing.

Item 20. As a minimum, all individuals should be interviewed prior to the start of Phase 2. This will give the team an idea of what vulnerabilities already have been identified and if there have been any corrective actions taken. You may have others you think should be interviewed to that end and those individuals may be added at "other."

Item 21. An organizational chart may assist you in compiling this list. You should include phone and email address and building/room number if available. This will assist you in assigning interviews and to ensure all appropriate staff members have been interviewed.

Item 22. There should be a complete list of survey team members, along with their contact information. You should provide this to every member of the team and include in the final report.

Item 23. Prepare an authorization letter for the Commander's signature; identify the purpose of the survey, the team member names and identification information, their clearance and the Commander's authority for them to conduct interviews. Team members should always carry it in case they are challenged or someone they are interviewing hesitates to cooperate. However, team members should only produce the letter when asked.

Item 24. Prepare a preliminary adversary strategy based on the team leader's assessment of adversaries to be included in the survey analysis. The adversary strategy identifies friendly objectives and possible strategies the adversary will use to defeat and/or mitigate friendly objectives or intentions.

Item 25. A process diagram must be prepared for the unit, mission, or operation being studied. The process diagram is simply a graphic representation of the processes performed by the studied organization and the means used to communicate with both internal and external organizations. The process diagram allows you to determine possible vulnerabilities.

Item 26. An optional page can be used for additional notes such as information and/or action items.

This page intentionally left blank.

APPENDIX F

OPSEC INTERVIEW CHECKLIST

Interviewee's Name/Unit: _____ Phone: _____
Interviewer(s): _____ Date/Time: _____

Section 1: Overview *Note: to interviewer: We want to know how well personnel understand OPSEC and their responsibilities.*					
Unless otherwise noted, use the appropriate unit scale for Section 1: 1) Very poor 2) Poor 3) Average 4) Good 5) Outstanding	1	2	3	4	5
1. What is operations security (OPSEC)? <u>Note to interviewer</u>. *Note whether the person can give you a reasonable explanation of OPSEC in general. Rate answer using the 1 to 5 scale below.* Criteria: 1 = No understanding. 2 = Confuses OPSEC with something else (i.e. COMSEC). 3 = Understands that OPSEC protects critical information 4 = Understands OPSEC principles, but may not use correct terminology. 5 = Fully understands the concepts of critical info, threat, vulnerability, risk, and countermeasures.					
2. Are you aware of your section/unit's OPSEC program? ☐Yes or ☐ No *Note to interviewer. If the person answers No, go on to question* 3. *If the answer is yes, ask the following:* How would you rate the OPSEC Program in terms of its contribution to mission success? 1 = Poor; 3 = Good; 5 = Excellent Why?:					
3. Does your section/unit have an OPSEC Coordinator? ☐Yes or ☐No <u>Note to interviewer</u>: *If the person answers no, go on to question 4. If the answer is yes ask the following.* How would you rate your section/unit in terms of getting you the information you need on OPSEC? Why?					
4. Have you received OPSEC training from this organization? ☐Yes or ☐No <u>Note to interviewer</u>. *If the person answers no, go on to section 2. If the answer is yes ask the following:* How would you rate the OPSEC training you have received? Why?					

Section 2: Individual Rating					
For Section 2 use the following scale: 1) Not at all 2) Slightly 3) Moderately 4) Mostly 5) Completely	1	2	3	4	5
1. OPSEC relates to my duties.					
2. I understand OPSEC sufficiently enough to employ its use.					
3. OPSEC receives sufficient emphasis in my section/unit.					
4. OPSEC receives sufficient emphasis in the organization.					
5. OPSEC is critical to the organization's mission.					

Section 3: Intelligence Threat

Note to interviewer. We need to determine how well the population understands the intelligence threat to their unit's/section's mission(s).

1. Programs that protect our information assume someone is out to get it. Do you believe there is a threat to THIS ORGANIZATION? ☐Yes or ☐No

Note to interviewer. If the person answers yes, ask the following.

Who (or what) do you think is a threat to the mission? (List countries, agencies, organizations, etc.) Please rate each as High or Medium or Low.

2. In OPSEC, threats are derived from adversaries. How do you think an adversary would collect or gather information about your section/unit's mission?

Note to interviewer. You may need to provide examples to demonstrate what you're talking about depending on the experience level of the interviewee. (i.e., monitoring of radio communications, foreigners soliciting information from you or your family, SATCOM, IMINT, etc.)

Section 4: Critical information
Note to interviewer. The objective is to determine how well individuals understand critical information.

1. What information about your mission/duties would an adversary want or need to know to be able to degrade or deny the mission? (use the adversary's point of view)

2. What information about your mission needs protection (from your point of view)?

3. When you are doing an exercise or an operation how does the information you need to protect change, or does it change?

Section 5: Information Processing (Computers)
Note to interviewer. We're looking for what systems are used to process information and whether or not those systems are encrypted or otherwise protected.

1. Do you use a computer at work? ☐Yes or ☐No
Note to interviewer. If No, go on to question 2. If yes:
What percentage of your time do you spend on a classified system?
On an unclassified system?

2. Do you use e-mail? ☐Yes or ☐No
Percentage classified _____Percentage unclassified _____
Do you use e-mail at home? ☐Yes or ☐No
Do you ever get business email at your home? ☐Yes or ☐No

3. Describe what you use your computer for; i.e. data base access, word processing, presentations, accessing Internet, etc.
Note to interviewer: We're especially interested in the various connections to other commands and/or national networks. Not interested in content!

4. Do you publish information on the world wide web (the Internet)? ☐Yes or ☐No
Any other web or Intranet? ☐Yes or ☐No
Do you provide personal or work-related information using internet based bulletin (Blogs) or websites? ☐Yes or ☐No
Note to interviewer. If necessary very briefly describe.

5. Do you get involved in publishing information of any kind on the web or internet? ☐Yes or ☐No
Explain:

6. What networks do you use in your job? (e.g. data base, web pages, SIPRNET, INTELINK)

7. Do you have NATO/COALITION/ALLIED interface? ☐Yes or ☐No

8. Do you use a laptop computer? ☐Yes or ☐No
Note to interviewer. If no, go on to question 10.
Is it encryption protected and approved for classified processing? ☐Unknown ☐Yes or ☐No
Is it government owned? ☐Yes or ☐No

9. Do you use any other personal communications equipment? ☐Yes or ☐No
If yes, describe: (Examples include pagers, palm pilots, GPS devices, etc.)
Note to interviewer. Do not include cell phones or radios in this answer.

Section 6: Telephones

1. What percentage of your phone calls each day are not secure?

2. Do you have ready access to a STU-III or STE? ☐Yes or ☐No
Note to interviewer. If No, go on to question 3. If Yes, ask the following:
Where is the phone located? (i.e., on your desk, in a common room, in another office)

Where is the crypto-ignition key (CIK) kept?

For CIKs kept in a safe, do you know the combination? ☐Yes or ☐No
How is the CIK controlled? (i.e., only taken out to use it or, loaded first thing, put away last, etc.)

3. Do you have ready access to any other secure phone? ☐Yes or ☐No

4. Please tell me some of the vulnerabilities of using a secure phone in an office where others are working in close proximity.
Note to interviewer. Don't give hints, but we're looking for 2 things: (1) an understanding that intelligence can be gleaned from discussions before and after going secure; (2) the possibility sensitive background conversations will be transmitted over the open line.

Section 7: Cell phones
1. Do you use a government owned cell phone? ☐Yes or ☐No If Yes, what are the vulnerabilities associated with cell phones? *<u>Note to interviewer</u>. Should discuss eavesdropping on activation, geo locating, and ease of interception.*
2. Do you use a personal cell phone? ☐Yes or ☐No If Yes, *Do* you use it for work? ☐Yes or ☐No Briefly what do you use it for? (non-attribution)
3. What if any, are the rules for bringing cell phones into work areas?
Section 8: Radios
1. Do you use a radio regularly for official business? ☐Yes or ☐No *<u>Note to interviewer</u>. If No, go to question 2. If yes, ask the following.* What do you use it for?
2. What are the vulnerabilities associated with radios? *<u>Note to interviewer</u>. Just looking for demonstrated understanding of radio vulnerabilities.*
Section 9: Fax
1. What percentage of faxes you send or receive are transmitted over non-secure lines?
2. Do you know how to get access to a secure fax? ☐Yes or ☐ No
Section 10: Other communications
1. Are there any other forms of communication that you use? ☐Yes or ☐No If yes, describe.

Section 11: Vulnerabilities

Note to interviewer. The objective is to understand the potential vulnerabilities within your organization.

1. How could an adversary get access to information you are trying to protect? (other than communications vulnerabilities already discussed)

2. Can you think of anything we do that would give an adversary clues about where to find critical information? If so, what would it be? ☐Yes or ☐ No

Note to interviewer. You may need to provide examples such as, mass leave cancellation, a rise in posted Force Protection level, extended hours of support functions, etc.

3. To your knowledge, are there known exploitations associated with any of the systems you are using? ☐Yes or ☐ No

Section 12: Training

1. What training have you received on the security of these communications systems?

Note to interviewer. You should reference the systems discussed earlier in this interview.

2. Please explain what "FOUO" is and are there any special handlings or destruction requirements?

Miscellaneous Notes

APPENDIX G

OPSEC SURVEY REPORT FORMAT (SAMPLE)

A. TABLE OF CONTENTS

Cover sheet (to be developed with organization)

B. EXECUTIVE SUMMARY

Who we are?
What we did?
What we learned?

C. INTRODUCTION

Background
Survey objective
What was the survey objective?
Was it to solve a known problem or was it to determine if there is a problem?

D. SURVEY CONSTRAINTS, LIMITATIONS AND BOUNDARIES

How was the survey bound so that it was manageable?
Did the resources exist to do the survey?
Where did the resources come from?
What was the urgency for the survey, if any?

E. SURVEY METHODOLOGY

Who were the key players in the sponsoring organization?
What type of support was required, i.e., red team, monitoring, etc.?
How was the OPSEC methodology applied?
- Looking at the activity from "Outside the box"
- Looking through the "Eyes of an adversary"
- Putting the "Puzzle together"

F. THREAT SUMMARY

The Adversary Strategy
- Who are they?
- What are their goals or objectives?
- What information do they need to meet their goals or objectives?
- How would the adversary go about collecting the information needed?
- What are their collection capabilities and limitations?

Possible Adversaries
International or domestic terrorists
Nation States
Countries

Threat Information
Unclassified Source
Classified "If applicable"

G. CRITICAL INFORMATION

Units
HHQ or Exercise/Operation Authority

H. OBSERVATIONS, DISCUSSIONS AND RECOMMENDATIONS

Critical information
Security
Communications
Operations
Public affairs
OPSEC awareness
Planning phase
Intelligence
Future exercises

I. CONCLUSIONS

Annex A—Forms
Annex B—Open Source Information

APPENDIX H

OPSEC REVIEW OF PAPER/PRESENTATION (EXAMPLE)

MEMORANDUM FOR RECORD

SUBJECT: Operations Security (OPSEC) Review of Paper/Presentation

1. The attached (paper, video, etc.) entitled (enter title here) dated (enter date of paper, video, etc.) is provided for review for public disclosure in accordance with (may want to insert DoD regulation versus Service regulation here). (Paper, video, etc.) is proposed for public release via (name and location of meeting, conference, symposium, publication, etc.).

2. I, the undersigned, am aware of the foreign intelligence interest in open source publications and in the subject matter of the information I have reviewed for OPSEC purposes. I certify that I have sufficient technical expertise in the subject matter of this paper, video, presentation, etc. and that, to the best of my knowledge, the net benefit of this public release outweighs the potential damage to the essential secrecy of all related ATC, TECOM, AMC, Army or other DOD programs of which I am aware.

	Name (Printed)	Signature	Date
Telephone Number of Author:	_____		

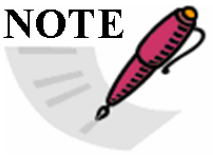
Concurrences

	Name (Printed)	Signature	Date
Program Manager/Customer (If not command-owned technology)	_____	_____	_____
Director	_____	_____	_____
Unit OPSEC POC	_____	_____	_____
OPSEC PM	_____	_____	_____
Public Affairs Officer	_____	_____	_____
Commander or Civilian Director (Return to PAO for further processing)	_____	_____	_____
HHQ GO/SES (If required by HHQ)	_____	_____	_____

This page intentionally left blank.

APPENDIX I

ANNUAL OPSEC REPORT FORMAT



The annual OPSEC report format is specified by each Service.

Example of an Annual OPSEC Report

MEMORANDUM FOR 45 SW OPSEC PM DATE

FROM: YOUR ORGANIZATION

SUBJECT: Annual OPSEC Self-Assessment Report

1.1 **OPSEC Initiatives/Projects/Successes**

a. Commander signed new policy letter dated in September with focus on specific OPSEC countermeasures to protect wing critical information.
b. Submitted request for OPSEC Survey on our cargo preparation procedures.
c. Published quarterly OPSEC articles in the base newspaper focusing on OPSEC indicators, threat, and countermeasures.
d. Provided $10K budget for wing OPSEC program management.

1.2 **OPSEC Training and Awareness**

a. Quarterly articles in base paper focusing on OPSEC.
b. Provided formal training for 2 wing PMs (AF OPSEC Course) and 4 of 8 squadron coordinators (IOSS 2380 course). All coordinators completed IOSS 1301 CBT.
c. Initial and refresher training accomplished across the wing. Created wing OPSEC awareness video and distributed to 100% of coordinators and POC within the wing.

1.3 **OPSEC in Operational Planning**

a. Wing OPSEC PM reviewed all base program plans, expeditionary site plans and deployment plans.
b. Conducted OPSEC working group to assist staff planning team to update appendix 3 of annex C of OPLAN 21-100.

1.4 **Assessment**

a. Developed OPSEC Master Scenario Events List (MSEL) injects for two base level exercises. Scenario's tested the effectiveness of OPSEC measures to reduce risk to deployment indicators. 23rd AS effectively concealed indicators by only conducting preparations inside hangers and moved supplies at night thus limiting exposure to possible adversary exploitation.

b. Wing successfully completed Operational Readiness Exercise with no findings for OPSEC. Best practice identified for training individuals on unit critical information, 100% of personnel questioned on unit critical information was able to identify and knew what information needed to be controlled.

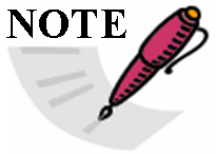
c. Conducted an OPSEC survey for the cargo preparation process with assistance from AFSPC OPSEC PM. Identified potential vulnerabilities within the process and implemented new procedures throughout the wing to reduce the vulnerabilities associated with preparation of cargo for deployments.

JAMES P. JAMISON, Col, USAF
Commander

APPENDIX J

MILITARILY CRITICAL TECHNOLOGIES LIST (MCTL)

The Militarily Critical Technologies List (MCTL) is a compendium of existing goods and technologies that DOD assesses would permit significant advances in the development, production, and use of military capabilities of potential adversaries. The MCTL home page containing the hyperlinks below can be seen at http://www.dtic.mil/mctl/MCTL.html.



As of publication date, the MCTL website has been temporarily removed with a re-establishment date to be determined.

File Size (kb)	Section (in pdf format)
215	Section 1 - Aeronautics Systems Technology
270	Section 2 - Armaments & Energetic Materials Technology
286	Section 3 - Chemical and Biological Systems Technology (for Revised Chemical Technology, see MCTL Revised, Section 5)
234	Section 4 - Directed and Kinetic Energy Systems Technology
374	Section 5 - Electronics Technology
263	Section 6 - Ground Systems Technology
155	Section 7 - Guidance, Navigation, and Vehicle Control Technology Section 7.1 Aircraft and Vehicle Control Systems (for Revised Navigation, Positioning, and Time technology, see MCTL Revised, Section 16)
273	Section 8 - Information Systems Technology (for Revised Information Security Technology, see MCTL Revised, Section 17)
389	Section 9 - Information Warfare Technology
	Section 10 - Processing and Manufacturing Technology (for Revised Processing and Manufacturing Technology, see MCTL Revised, Section 12)
441	Section 11 - Materials Technology
160	Section 12 - Marine Systems Technology
266	Section 13 - Nuclear Systems Technology
313	Section 14 - Power Systems Technology
209	Section 15 - Sensors and Lasers Technology
	Section 16 - Signature Control Technology , [READ ME FIRST] (for Revised Signature Control Technology, see MCTL Revised, Section 18)

APPENDIX K

DOD DISTRIBUTION STATEMENTS

(Use appropriate distribution statement)

The following distribution statements are authorized for use on DOD technical documents:

a. Distribution Statement A. Approved for public release; distribution is unlimited.

b. Distribution Statement B. Distribution authorized to U.S. Government agencies only (fill in blank, e.g. Foreign Government Information, Proprietary Information, Test and Evaluation, Contractor Performance Evaluation, Administrative or Operational Use, Software Documentation, or Specific Authority) (date of determination). Other requests for this document shall be referred to (insert controlling DOD office).

c. Distribution Statement C. Distribution authorized to U.S. Government agencies and their contractors (fill in reason, e.g. Critical Technology, Administrative or Operational Use, or Specific Authority) (date of determination). Other requests for this document shall be referred to (insert controlling DOD office).

d. Distribution Statement D. Distribution authorized to the Department of Defense and DoD contractors only (fill in reason, e.g. Premature Dissemination, Software Documentation, Critical Technology, or Specific Authority) (date of determination). Other requests for this document shall be referred to (insert controlling DOD office).

e. Distribution Statement E. Distribution authorized to DOD Components only (fill in reason, e.g. Export Limitations, Foreign Government Information, Premature Dissemination, Software Documentation, Critical Technology, or Specific Authority) (date of determination). Other requests for this document shall be referred to (insert controlling DOD office).

f. Distribution Statement F. Further dissemination only as directed by (insert controlling DOD office) (date of determination) or higher DOD authority.

g. Distribution Statement X. Distribution authorized to U.S. Government agencies and private individuals or enterprises eligible to obtain export-controlled technical data in accordance with regulations implementing 10 U.S.C. 140c (date of determination). Other requests must be referred to (insert controlling DOD office).

This page intentionally left blank.

APPENDIX L

RECOMMENDED CONTENTS FOR OPSEC PLAN

The OPSEC plan format is Service-specific. However, plans should generally include the following information:

a. References.

b. General Mission/Program Description.

c. Security Responsibilities.

d. Critical Information List (CIL).

e. Indicators.

f. Threat.

g. Vulnerabilities.

h. Countermeasures and Risk Assessment.

i. Commander's or Director's decision on which risks to accept and which countermeasures to implement.

j. Public Affairs.

k. Training.

l. Supporting Units/Associated Programs.

m. Resources Utilized.

This page intentionally left blank.

APPENDIX M

SAMPLE MATERIAL SECURED RECYCLING PLAN

Revision Date:XXXXXX
Material Recycling Facility (MRF) Security Plan

Contract Number:	**XXXXXXX**
Contract:	XXXXXXX Recycling Program
Contractor:	XXXXXXX

This facility security plan will be a process to facilitate securing the commodities collected from exposure to unauthorized persons. Primarily this plan is directed towards securing paper collected that could contain sensitive but unclassified material. This would include any FOU, FOUO, HIPPA, and other sensitive issues (Reference: DoD5205.2m.)

1.1 Vehicles

The security process begins with retrieving the commodities at the individual facilities. Trucks will remain locked with the windows closed at all times unless loading or unloading commodities from the back of the truck. When the truck is unlocked and/or open, it will always have a XXXXXX representative near it watching over the vehicle and commodities.

All trucks departing the MRF with sensitive recycled material will be locked and sealed with an appropriate security seal. (See Secure White Paper Procedures for more details.)

1.2 Gates

The gate will remain locked at all times unless a customer arrives with oil to be pumped out.

The main gate to the MRF will remain closed and signs notating No Authorized Entry will be posted frequently along the fence. This gate will be locked only at night when no personnel are present. Signs directing personnel to check in at the front office are posted.

Authorized personnel will be allowed through the gate by a XXXXXX representative and assisted as necessary to retrieve the commodities or to provide service and maintenance.

1.3 Door at the Material Recycling Facility (MRF)

Rollup bay doors for the white paper and office waste will remain closed and secured at all times except when the commodities are being stored or being prepped for shipping.

Doors leading to the outside from the can crushing room and the can sorting room will remain closed and locked except as and emergency exit. Signs are posted on these doors for Emergency Exit Only.

Main entrance door to the MRF is self locking. A door bell has been installed for customer assistance. Signs on the door are posted, No Unauthorized Entry; Ring Door Bell for Service.

1.4 Commodities

If it is found that paper containing information above sensitive but unclassified (Reference: DoD 5202.02-M) was inadvertently placed in the recycling bin, the possible classified material will be brought to the attention of the Project Manager or MRF Supervisor and the following procedure would be followed once it is discovered:

a. The potentially Classified Information will be identified, secured and protected at all times.
b. Simultaneously, the bay doors to the main building will be shut and XXXXXX Information Protection Office (XXXPhoneXXX)) or Security Forces (XXXPhoneXXX) will be notified of the breach and asked to secure the facility.
c. No Personnel except Security will be allowed to enter or exit the facility. XXXXXX employees and any other service personnel will be directed into the break room to wait for further instructions. These personnel will only be allowed to leave the break room to use the restroom immediately outside the break area.
d. The XXX OPSEC Program Manager will be contacted (XXXPhoneXXX) and made aware of the breach and advised of the steps being taken to contain the information. XXXXXX contractor will then wait for further instructions from XXXXXX OPSEC and XXXXXXInformation Protection Office.
e. The QRP Manager will be contacted (XXXPhoneXXX) and made aware of the breach and advised of the steps being taken.

1.5 Sign In/Sign Out Procedure

All Customers and Service personnel who visit the MRF, and require entrance into the gated area or the main building will be required to sign in and out.

1.6 Key Control

The number of keys to the facility will be kept to a minimum and logged for auditing purposes. At this time only the following positions have a key to access the facility: Quality Recycle Program (QRP) Manager, Project Manager, MRF Supervisor and the three (3) Crew Leaders.

APPENDIX N

INFORMATION PROTECTION WALK-THRUS AND RECEPTACLE INSPECTIONS

EXAMPLE:

1.1 Concept of Operations

1.1.1 Synopsis**.** The following is the Concept of Operations (CONOPs) for conducting Information Protection walk-thrus and receptacle inspections for the XXXAgencyXXX. This program is one of many tools used to protect critical and sensitive information throughout the XXXAgencyXXX and its tenant units.

1.1.2 Background. The protection of information is an essential security measure personnel sometimes take for granted. With the explosion of technology and the steadily increasing accessibility to critical information, the protection of information is becoming more and more challenging every day. To properly protect information we must incorporate a multifaceted approach of education, system counter measures, proper and current guidance, and physical inspections. The receptacle inspections will be a portion of the physical inspections conducted within XXXAgencyXXX. These types of active inspections in concert with OPSEC, Security Manager training and Information Security Program Reviews will enhance the 45 Space Wing's ability to protect its information and mission.

1.1.3 CONOPS**.** Each organization with membership in the XXXAgencyXXX will be scheduled within a 12 month period to participate in the walk thru and receptacle inspections program. The representative will have their AF FM 55 documented with this task and will be required to complete Blood-borne Pathogen and Self Aid Buddy care training annually. Inspections will be conducted as follows:

a. All inspections will be conducted monthly during normal duty hours, however can be conducted after duty hours at the unit's discretion. Inspections will be IAW the current schedule. (See Attachment 1/Inspection Schedule and Attachments 5-XXX for Maps).
b. It is the responsibility of the organization scheduled to contact the organizing agency at XXXPhoneXXX to coordinate the inspections for their scheduled month IAW inspection procedures. (See Attachment 2/Inspection Procedures). Each responsible agency will select personnel from their respective unit and have them contact the for instructions. The representative will provide program guidance and a safety briefing to all personnel conducting the inspections and IAW the Safety brief (See Attachment 3/safety brief) and have the inspectors sign the form.
c. Once the inspections are complete the report will be drafted IAW report template, (See Attachment 4/Report Template) reviewed, and sent to the XXXAgencyXXX. Contact the organizing agency if you have any questions concerning the report.

d. Units will have 30 calendar days to conduct the inspection, complete the report, and submit the report to the XXXAgencyXXX.
e. The report will be sent to the XXXAgencyXXX/CV for review and action if applicable. The ***non-specific*** report will be briefed monthly at the mission partners wing stand-up the following month.
f. If during an inspection classified information or possible classified information is found discarded or unprotected the inspection will stop immediately and the XXXAgencyXXX/ representative will perform required actions to secure the classified material/information.
g. The XXXAgencyXXX/ representative will take charge of the information or materials found, make all required notifications and initiate the necessary procedures IAW with a possible Security Incident.

Attachment 1
WALK-THRUS AND RECEPTACLE INSPECTION SCHEDULE

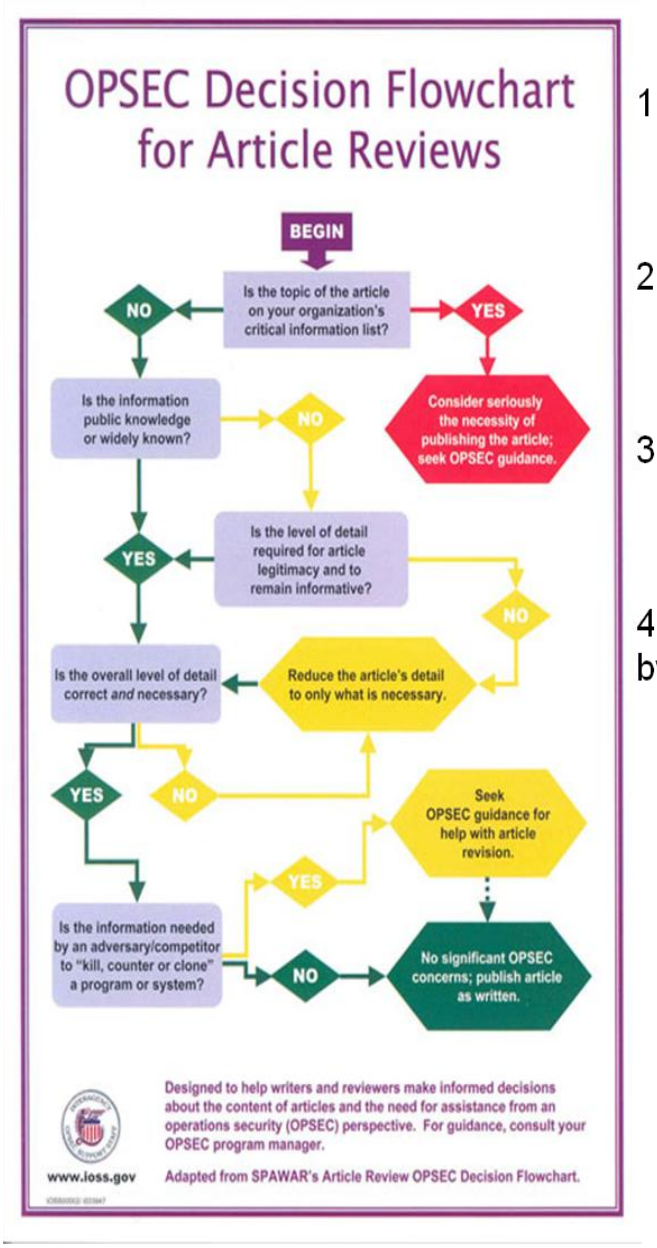
<<<<<<<<Put your annual schedule of inspections here>>>>>>>

APPENDIX O

REVIEW PROCESS

1.1 Document Review Process

The following diagram describes the document review process.



1. Is the info on the CIL?
   a. Is it required by the treaty?
   b. If not then consider redacting.

2. Is the info open source?
   a. Is it required by the treaty?
   b. If not then consider redacting.

3. Is the level of detail required?
   a. Is it required by the treaty?
   b. If not then consider redacting.

4. Is the info valuable or needed by a threat?
   a. Is it required by the treaty?
   b. If not then consider redacting.

1.2 Personnel Interview Process

The following sub-paragraphs describe the personnel interview process.

1.2.1 Pre-Interview Guidance.

a. Nature/Context of request.
   - [Insert as specific information is available]

b. Appropriateness of request.
   - [Insert when available, as based on interviewee scope of responsibility/area of expertise]

c. Anticipated topics/line of questioning.
   - [Insert current guidance when available]

d. Procedural guidance.
   - [Insert any information regarding procedures when available]

1.2.2 Interview Response Guidance.

a. Answer with information directly related to Inspection Mandate.
   - If in doubt, speak to a representative before answering

b. Be specific and as brief as possible.
   - Do not volunteer information not requested.
   - Do not provide information outside your current responsibilities.

c. Do not reveal classified, proprietary, or sensitive information.
   - Speak to a representative if asked about such information.

d. Do not speculate.
   - If you don't know the answer, say you don't know.
   - Do not answer hypothetical questions.

e. Do not appear hesitant or evasive.
   - If you can't answer, be straightforward as to why.

1.2.3 Interviewee Rights.

a. Right to decline interview request.

b. Right to decline to answer specific questions.

c. Right to consult with U.S. representative and/or attorney.
   - Representatives will be present and available during interview.
   - Interview can be stopped as necessary for consultation.

d. Interviews not recorded (video or audio).
   - Note-taker will be present.

APPENDIX P

DOCUMENT REVIEW PROCESS LETTER

Range Commanders Council

SECRETARIAT

Document Number: _____
(To be assigned by RCC Secretariat)

SUBJECT: Operations Security (OPSEC) Review of RCC Document

REPLY TO: RCC Secretariat
ATTN: TEDT-WS-RCC
White Sands Missile Range, NM 88002-5110
Phone: 575-678-1107
Fax: 575-678-7519

Document Title: _____

_____

The above named document has been reviewed for OPSEC implications by both a Subject Matter Expert (SME) and an OPSEC Officer. The appropriate RCC Distribution Statement is:

	DISTRIBUTION STATEMENT A: Approved for public release; distribution is unlimited.
	DISTRIBUTION STATEMENT C. Distribution authorized to U.S. Government Agencies and their contractors (fill in reason) (date of determination). Other requests for this document shall be referred to (insert controlling DoD office)
	DISTRIBUTION STATEMENT D. Distribution authorized to the Department of Defense and U.S. DoD contractors only (fill in reason) (date of determination). Other requests shall be referred to (insert controlling DoD office).
	INTERNAL RCC DISTRIBUTION. Distribution authorized to internal Range Commanders Council (RCC) membership only.

The attached document **does not** contain Classified Information, Critical Information (CI) or Essential Elements of Friendly Information (EEFI), information considered Operationally Sensitive to DoD activities, For Official Use Only (FOUO), or technical information protected under the Military Critical Information List (MCTL).

I, the undersigned, am aware of hostile intelligence interest in DoD operations, open source information, and have sufficient technical knowledge of the subject matter to competently review and approve this information for release as approved. I certify the information contained does not violate OPSEC tenets and regulatory guidance, and the net benefit of this public release outweighs the potential damage to the essential secrecy of our operations. Moreover, the release of this document will not be a detriment to the National Security of the United States.

DATE

SME PRINTED NAME

SME SIGNATURE

TITLE

ADDRESS

PHONE DSN FAX

OPSEC REVIEWER'S PRINTED NAME

OPSEC REVIEWER'S SIGNATURE

TITLE

ADDRESS

PHONE DSN FAX

GLOSSARY

Acceptable Level of Risk. An authority's determination of the level of potential harm to an operation, program, or activity due to the loss of information that the authority is willing to accept.

Acquisition Program. A directed and funded effort that is designed to provide a new, improved, or continuing weapons system or automated information system capability in response to a validated operational need.

Adversary. An individual, group, organization, or government that must be denied critical information. Synonymous with competitor/enemy.

Adversary Collection Methodology. Any resource and method available to and used by an adversary for the collection and exploitation of sensitive/critical information or indicators thereof.

Analysis. The process by which information is examined in order to identify significant facts and/or derive conclusions.

Assessment. To evaluate the worth, significance, or status of something; especially to give an expert judgment of the value or merit of something.

Blog. The term universally used for "weblog", a type of website where entries are made (such as in a journal or diary), and displayed in a reverse chronological order.

Countermeasure. Anything which effectively negates or mitigates an adversary's ability to exploit vulnerabilities.

Counterintelligence (CI). Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities.

Critical Information. Specific facts about friendly intentions, capabilities, and activities vitally needed by adversaries for them to plan and act effectively to guarantee failure or unacceptable consequences for friendly mission accomplishment.

Critical Information List (CIL). Those areas, activities, functions, or other matters that a facility/organization considers most important to keep from adversaries.

Critical Program Information (CPI). Information, technologies, or systems that, if compromised, would degrade combat effectiveness, shorten the expected combat-effective life of the system, or significantly alter program direction. This includes classified military information or unclassified controlled information about such programs, technologies, or systems.

Freedom of Information Act (FOIA). A provision that any person has a right, enforceable in court, of access to federal agency records, except to the extent that such records (or portions thereof) are protected from disclosure by one of nine exemptions.

Information Operations (IO). Actions taken to affect adversary information and information systems while defending one's own information and information systems.

Multi-disciplined Vulnerability Assessment (MDVA). A systematic analytical process performed to assess an installation's application of influence operations and security processes to determine specific vulnerabilities. MDVAs simulate various IO threats to identify an installation or organization's vulnerabilities (OPSEC, network, physical security, etc.), operational impacts if those vulnerabilities are exploited and exercise response procedures to the simulated threat. Identifies areas of improvement to withstand, mitigate, or deter acts of violence, terrorism, sabotage, or espionage.

Observables. Any actions that reveal indicators which are exploitable by adversaries.

Operations Security (OPSEC). A process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to: a. identify those actions that can be observed by adversary intelligence systems; b. determine indicators that hostile intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries; and c. select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation.

OPSEC Assessment. A thorough evaluation of the effectiveness of a customer's implementation of OPSEC methodology, resources, and tools. Assessments (a) are used to evaluate the effectiveness of the customer's corporate level OPSEC program and (b) can be used at the program level to determine whether a program is a viable candidate for an OPSEC survey.

OPSEC Coordinator. Below the appropriate unit level. Acts as an interface to direct and manage all relevant OPSEC matters. Reports to OPSEC Program Manager

OPSEC Program Manager. At the appropriate unit level. Focal point for OPSEC related matters and ensures OPSEC requirements are in compliance as directed from Higher Headquarters. Reviews operations plans to ensure a statement of OPSEC considerations and appropriate guidance regarding Critical Information are included.

Operations Security Indicator. Any detectable activity and/or information that, when looked at by itself or in conjunction with something else, allows an adversary to obtain critical or sensitive information.

Operations Security Process. An analytical process that involves five components: identification of critical information, analysis of threats, analysis of vulnerabilities, assessment of risks, and application of appropriate countermeasures (NSC 1988).

Operations Security Program. An OPSEC program is the vehicle by which the principles and practices of OPSEC are employed within an organization.

Operations Security Survey. The application of OPSEC methodology at the program level. It is a detailed analysis of all activities associated with a specific operation, project, or program in order to determine what exploitable evidence of classified or sensitive activity could be acquired in light of the known collection capabilities of potential adversaries.

Operations Security Working Group (OWG). A (normally formally) designated body representing a broad range of line and staff activities within an organization that provides OPSEC advice and support to leadership and all elements of the organization.

Risk. A measure of the potential degree to which protected information is subject to loss through adversary exploitation.

Risk Analysis. A method by which individual vulnerabilities are compared to perceived or actual security threat scenarios in order to determine the likelihood of compromise of critical information.

Risk Assessment. An OPSEC process of evaluating the risks of information loss based on an analysis of threats to, and vulnerabilities of, a system, operation, or activity.

Sensitive Information. Information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under 5 U.S.C. Section 552a (the Privacy Act), but that has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy (NSTISSI 1997).

Special Access Program. A program established for a specific class of classified information that imposes safeguarding and access requirements that exceed those normally required for information at the same classification level (NSC EO 1995).

Threat. The capability of an adversary coupled with his intentions to undertake any actions detrimental to the success of program activities or operations.

Threat Analysis. An OPSEC process, which examines an adversary's technical and operational capabilities, motivation, and intentions, designed to detect and exploit vulnerabilities.

Threat Assessment. An evaluation of the intelligence collection threat to a program activity, system, or operation.

Vulnerability. A condition in which friendly actions provide OPSEC indicators that may be obtained and accurately evaluated by an adversary in time to prove a basis for effective adversary decision making.

Vulnerability Analysis. In information operations, a systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation. See also information operations; information system; security; vulnerability.

Vulnerability Assessment. An evaluation (assessment) to determine the vulnerability of an installation's application of influence operations and security processes to determine specific vulnerabilities. Identifies areas of improvement to withstand, mitigate, or deter acts of violence, terrorism, sabotage, or espionage.

**** NOTHING FOLLOWS ****