U.S. Department of Homeland Security

United States Coast Guard

OPERATIONS SECURITY (OPSEC) PROGRAM

COMDTINST M5510.24A

U.S. Department of Homeland Security
United States Coast Guard

Commandant
United States Coast Guard
Office of Security Policy
and Management

2703 MARTIN LUTHER KING JR AVE SE
Stop 7202
WASHINGTON DC 20593-7202
Staff Symbol: DCMS-34
Phone: (202) 372-3700
Fax: (202) 372-3950

COMDTINST M5510.24A
22 April 2014

COMMANDANT INSTRUCTION M5510.24A

Subj: COAST GUARD OPERATIONS SECURITY (OPSEC) PROGRAM MANUAL

Ref: (a) National Security Decision Directive (NSDD) 298, "National Operations Security Program," January 22, 1988
(b) 32 CFR Parts 2001 and 2003, Classified National Security Information; Final Rule
(c) Executive Order 13526, Classified National Security Information
(d) Executive Order 13556, Controlled Unclassified Information
(e) Department of Homeland Security (DHS) Management Directive Number 11042.1, Safeguarding Sensitive but Unclassified (FOUO) Information
(f) Department of Homeland Security (DHS) Management Directive Number 11056.1, Sensitive Security Information
(g) Department of Homeland Security (DHS) Management Directive Number 11080, Security Line of Business Integration and Management
(h) Department of Homeland Security (DHS) Management Directive Number 11060.1, Operations Security Program
(i) Classified Information Management Program, COMDTINST M5510.23 (series)
(j) Security and Information Assurance Manual, COMDTINST M5500.13 (series)
(k) Telecommunication Manual, COMDTINST M2000.3 (series)
(l) Communications Security (COMSEC) Monitoring, National Telecommunications and Information Systems Security Directive Number 600 [NTISSD No. 600]
(m) Telecommunications TTP, CGTTP-6-01.2

DISTRIBUTION – SDL No. 163

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
A	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X		X		X					
B	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
C	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
D	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X			X
E	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X		X	X	X				X	X		
F																	X	X	X	X						
G		X	X	X	X																					
H																										
I																										

NON STANDARD DISTRIBUTION

1. PURPOSE. This Manual prescribes the policies and procedures and assigns responsibilities for the United States Coast Guard (USCG) OPSEC Program. The purpose of the USCG OPSEC Program is to promote operational effectiveness, and reduce risk by identifying, controlling, and protecting primarily unclassified evidence of the planning and execution of sensitive activities.

2. ACTION. Area and district commanders, commanding officers of headquarters units, assistant commandants for directorates, Judge Advocate General, and special staff offices at Headquarters shall ensure compliance with the provisions of this Instruction. Internet release is authorized.

3. DIRECTIVES AFFECTED. The Operations Security Program, COMDTINST M5510.24, is hereby cancelled.

4. DISCLAIMER. This guidance is not a substitute for applicable legal requirements, nor is it itself a rule. It is intended to provide operational guidance for Coast Guard personnel and is not intended to nor does it impose legally-binding requirements on any party outside the Coast Guard.

5. MAJOR CHANGES. Major changes to this manual include the addition of: updated DCMS-34 OPSEC Program Manager responsibilities; updated Area/District OPSEC Coordinator responsibilities; updated unit OPSEC Coordinator responsibilities; updated which units are required to have an OPSEC Coordinator appointed in writing; a critical information list; an OPSEC resources section; updated indicators section; updated countermeasures section; updated OPSEC Program self assessment checklist; updated OPSEC Activities Annual report; and an OPSEC support request section.

6. IMPACT ASSESSMENT. The update of OPSEC Coordinator tasks in this manual require no new resources. Workload for OPSEC Coordinators remains the same as COMDTINST M5510.24. OPSEC Coordinator “C” training will continue to be funded by AFC-56.

7. ENVIRONMENTAL ASPECT AND IMPACT CONSIDERATIONS.

    a. The development of this Manual and the general policies contained within it have been thoroughly reviewed by the originating office in conjunction with the Office of Environmental Management, and are categorically excluded (CE) under current USCG CE # 33 from further environmental analysis, in accordance with Section 2.B.2. and Figure 2-1 of the National Environmental Policy Act Implementing Procedures and Policy for Considering Environmental Impacts, COMDTINST M16475.1 (series). Because this Manual contains guidance on, and provisions for, compliance with applicable environmental mandates, Coast Guard categorical exclusion #33 is appropriate.

b. This directive will not have any of the following: significant cumulative impacts on the human environment; substantial controversy or substantial change to existing environmental conditions; or inconsistencies with any Federal, State, or local laws or administrative determinations relating to the environment. All future specific actions resulting from the general policies in this Manual must be individually evaluated for compliance with the National Environmental Policy Act (NEPA), DHS and Coast Guard NEPA policy, and compliance with all other environmental mandates. Due to the administrative and procedural nature of this Manual, and the environmental guidance provided within it for compliance with

all applicable environmental laws prior to promulgating any directive, all applicable environmental considerations are addressed appropriately in this Manual.

8. DISTRIBUTION. No paper distribution will be made of this Manual. An electronic version will be located on the following Commandant (CG-612) web sites. Internet: http://www.uscg.mil/directives/, and CGPortal: https://cgportal2.uscg.mil/library/directives/SitePages/Home.aspx.

   NOTE: If paper copies are required please complete Certificate for Need of Printing, DHS Form 500-07, which can be found at http://www.uscg.mil/directives/Printing_Graphics.asp.

9. RECORDS MANAGEMENT CONSIDERATIONS. This Manual has been evaluated for potential records management impacts. The development of this Manual has been thoroughly reviewed during the directives clearance process, and it has been determined there are no further records scheduling requirements, in accordance with Federal Records Act, 44 U.S.C. 3101 et seq., National Archives and Records Administration (NARA) requirements, and the Information and Life Cycle Management Manual, COMDTINST M5212.12 (series). This policy does not have any significant or substantial change to existing records management requirements.

10. FORMS/REPORTS. None.

11. REQUEST FOR CHANGES. Units and individuals may recommend changes via the chain of command to: HQS-DG-lst-DCMS-34@uscg.mil.

M. K. BROWN /s/
Vice Admiral, U.S. Coast Guard
Deputy Commandant for Mission Support

TABLE OF CONTENTS

THE UNITED STATES COAST GUARD
OPERATIONS SECURITY (OPSEC) PROGRAM

A. PURPOSE. This Manual prescribes the policies and procedures, and assigns responsibilities for the United States Coast Guard Operations Security (OPSEC) Program. The purpose of the USCG OPSEC Program is to promote operational effectiveness and reduce risk by identifying, controlling, and protecting generally unclassified information on the planning and execution of sensitive activities.

B. BACKGROUND. A wide range of security policies and programs are currently enforce to protect classified information and operations. However, information generally available to the public as well as certain detectable activities reveal the existence of, and sometimes details about, classified or sensitive information or operations. These indicators represent a significant risk to USCG security. An adversary may be able to exploit the vulnerabilities identified in these activities through readily available information, and thereby effectively target and disrupt USCG operations. The OPSEC process is designed to address the vulnerabilities inherent in detectable indicators of friendly activities and apply appropriate countermeasures. OPSEC is the security practice that complements the traditional security disciplines (Physical, Communications, Personnel, Industrial and Information Security) and is a critical element of any comprehensive security program.

C. APPLICABILITY. This Manual applies to all United States Coast Guard organizations, personnel, and contractors that use or have access to details about USCG activities, operations, capabilities, and intentions. Coast Guard personnel are also actively encouraged to share the concepts contained herein with their family members as they too can contribute immeasurably to the overall Coast Guard OPSEC effort by judicious application of OPSEC principles.

D. TERMS AND ABBREVIATIONS. See Enclosure 1.

E. AUTHORITY. In 1988, President Ronald Reagan signed National Security Decision Directive (NSDD) 298, National OPSEC Program. This directive mandates that each Executive department and agency assigned or supporting national security missions with classified or sensitive activities shall establish a formal OPSEC program

F. THREAT. The multi-mission nature of the United States Coast Guard, which includes maritime law enforcement functions, homeland security, border and national defense, brings with it a broad range of operational activities and a corresponding range of potential adversaries. Those adversaries include fishermen operating outside the law, smugglers, insider threats, Foreign Intelligence Entities (FIE), and terrorists. Each of these adversaries has some capability to observe and monitor USCG activities and operations, and to assess USCG vulnerabilities using the information gained from such collection activities. While some may use this information merely to evade detection and avoid prosecution, others can and have demonstrated the capability to direct hostile action against U.S. ships, installations, and personnel. The inherent risks of an open and free society, where information is readily available to the public; the proliferation of open source information via all forms of news media and the internet; and the ready availability of sophisticated electronic monitoring devices that

permit eavesdropping of communications and electronic signatures have all contributed to a dramatic rise in the potential threat to USCG operations.

G. OPSEC DEFINITION. OPSEC is an analytical process used to deny an adversary information (generally unclassified) concerning our intentions and capabilities by identifying, controlling, and protecting indicators associated with our planning processes or operations.

H. OPSEC PROCESS.

1. The OPSEC Process consists of five interrelated steps. It is a methodology designed to guide the user through a series of steps to identify critical information and OPSEC indicators, and develop countermeasures to mitigate vulnerabilities inherent to the critical information. The five steps are as follows:

   a. Identify Critical Information: Determine what information is available to an adversary that could be used to target the organization or the unit's ability to effectively carry out a particular operation. This critical information constitutes those pieces of information that are central to the mission's success. The USCG Critical Information List (CIL) is provided in Enclosure 2. Although some critical information is classified when pertaining to national security issues such as military or intelligence operations, still other unclassified information is not afforded the same protection. It is this unclassified information, or indicators thereof, which, when considered in aggregate, may provide an adversary with clues to other more critical data. Indicators are data derived from open (unprotected) sources or detectable actions. These indicators may be prevalent in our daily routines, such as administrative, operational and logistical activities. A comprehensive listing of these indicators is provided in Enclosure 3.

   b. Analyze the Threat: Knowing who the adversaries are and what information they require to meet their objective(s) is essential in determining what information is truly critical. In any given situation, there is likely to be more than one adversary and each may be interested in different types of information. The adversaries' ability to collect information using the full range of intelligence disciplines must be considered: Human Intelligence (HUMINT), Signals Intelligence (SIGINT), Imagery Intelligence (IMINT), Measurement and Signature Intelligence (MASINT), Acoustic Intelligence (ACINT), Telemetry Intelligence (TELINT), and Open Source Intelligence (OSINT). We must also consider their ability to process and analyze that information, as well as their **intention and capability** to pose a credible threat. If any element of this threat analysis is missing, the threat is eliminated. For example, a group that desires information contained in encrypted radio transmissions, but does not have the *capability* to obtain it, is not a threat, while a group that desires to know when a cutter or aircraft departs its unit, and can observe it, is surely a threat. The objective, therefore, of threat analysis is to know as much as possible about each adversary and the strategies/options available to them for targeting the unit and its operations. It is also important to analyze the adversarial threat within the context of

the actual operation and, to the extent possible, determine what the adversaries' capabilities will be for the specific time and location of the Coast Guard operation.

c. Analyze Vulnerabilities: Determining vulnerabilities involves conducting a detailed analysis of how an operation is normally conducted. The operation must be viewed from the adversarial perspective. An OPSEC vulnerability exists when the adversary is capable of collecting critical information or indicators, analyzing it, and then acting quickly enough to impact friendly objectives.

d. Assess Risk: According to the Central Intelligence Agency (CIA) model, a Risk Assessment is "the process of evaluating the risks of information loss based on an analysis of threats to, and vulnerabilities of, a system, operation or activity." In mathematical terms, a risk formula looks like this:

Risk = Threat x Vulnerability x Impact

In order to assess risk to an asset (e.g., information, property and/or people) three conditions must be present: (1) one or more vulnerabilities, (2) a threat, and (3) an impact or consequence. The absence of a threat or vulnerability removes the risk. The absence of an identified consequence does not in every case eliminate risk but certainly does mitigate it, (i.e. make it more acceptable). Vulnerabilities and threats must be correlated. Where a unit's vulnerabilities are exploitable and enemy capabilities and intentions are present, the risk of adversarial exploitation must be anticipated. Therefore, a higher priority for protection needs to be assigned and countermeasures applied. Conversely, where the vulnerability is moderate or slight and the adversary has a limited collection capability, the priority may be medium to low.

e. Apply Countermeasures: Appropriate cost-effective countermeasures to minimize or mitigate vulnerabilities, threats, and the utility of critical information to adversaries must be developed. These countermeasures must be designed to defeat or delay adversarial actions to a point of acceptable risk. Countermeasures may include procedural changes, suppression of indicators to deny critical information, deception, perception management, intelligence countermeasures, traditional security measures, or any other action that is likely to work in a given situation. There are no standard solutions for all circumstances. This dynamic process requires continual evaluation and creativity. Periodic evaluation of countermeasures is not only required to assess their continual effectiveness, but also to determine if the countermeasures themselves have become an indicator. Perhaps the most cost-effective measure a unit can take is to adopt an active training and awareness program. Clear guidance from the command regarding what can and cannot be discussed outside the confines of the unit can have a significant impact on overall security. By their nature, some countermeasures may only be useful once or twice, while others may be effective on a long-term basis. The Commanding Officer must determine which countermeasures

are appropriate and cost-effective based on the results of the Risk Assessment. Enclosure 4 provides a list of potential countermeasures.

I. RESPONSIBILITIES.

1. Commandant (DCMS-34): Office of Security Policy and Management (DCMS-34) is the Office of Primary Responsibility for the USCG OPSEC Program and assigns a USCG OPSEC Program Manager (PM) from the DCMS-341 Staff. The USCG OPSEC PM will perform the following:

   a. Serve as the focal point for all USCG OPSEC Program Management by providing advice and assistance to field OPSEC Coordinators regarding OPSEC program development, including marketing, awareness, training, compliance, and assessment.

   b. Appoint an OPSEC Coordinator as an alternate to the OPSEC Program Manager. The OPSEC Coordinator assists in the development, organization, and administration of the OPSEC Program. In addition, the OPSEC Coordinator also assists in the integration, coordination, and synchronization of subordinate OPSEC programs.

   c. Represent USCG on the Department of Homeland Security (DHS) OPSEC Working Group.

   d. Establish procedures and facilitate USCG interagency and intra-agency coordination for OPSEC.

   e. Monitor and inspect USCG compliance with OPSEC Training and Awareness Standards outlined in this Manual, applicable DHS directives, and the Interagency OPSEC Support Staff (IOSS) guidelines.

   f. Establish USCG OPSEC reporting requirements and prepare the USCG Annual OPSEC Review for submission to DHS (Enclosure 6).

   g. Actively promote (market) the OPSEC concept through innovative media (i.e. posters) and other information sources, as well as effective training programs.

   h. Maintain the OPSEC SharePoint sub-site on DCMS-34's SharePoint site: http://hqs-spweb10-001:10116/sites/DCMS34/opsec.

   i. Provide student names for attendance to the OPSE-2500 Program Management and Analysis C-school course to Force Command (FORCECOM).

   j. Recommend changes to USCG OPSEC policy, procedures, and practices. To accomplish this, revise and update this Manual as necessary in accordance with OPSEC best practices, USCG operational needs, Department of Homeland Security (DHS) guidelines, and National Policy.

2. Public Affairs (CG-092): Ensure that the OPSEC Process is incorporated into public affairs activities.

3. Engineering and Logistics (CG-4): Ensure that the OPSEC Process is incorporated into the Engineering, Logistics and Resource Programs (i.e. Civil Engineering activities that reveal critical infrastructure information).

4. Acquisition (CG-9):

   a. Ensure that the OPSEC Process is applied to all acquisition programs, and contracts that support those programs.

   b. Ensure that the OPSEC Process is applied to all Research, Development Testing and Evaluation (RDT&E) efforts.

5. Human Resources (CG-1): Ensure that an initial OPSEC orientation is incorporated into the in-processing procedures for new civilian employees and those persons detailed from other services (i.e., health professionals, U.S. Public Health Service (USPHS) officers, Clergy, U.S. Navy chaplains and other detailees).

6. Intelligence & Criminal Investigations (CG-2):

   a. Designate an OPSEC Coordinator in writing and provide the name of that responsible person to the Office of Security Policy and Management (DCMS-34).

   b. Provide threat assessment support to facilitate OPSEC planning by OPSEC Coordinators.

7. Command, Control, Communications, Computers & IT and CG Cyber Command (CG-6/CYBERCOM):

   a. Designate an OPSEC Coordinator in writing and provide the name of that responsible person to the Office of Security Policy and Management (DCMS-34).

   b. Ensure compliance with the provisions of this Manual by incorporating sound OPSEC principles into all operational planning and activities.

   c. Ensure that the OPSEC Process is incorporated into Enterprise Architecture and Configuration Management Activities.

8. Deputy Commandant for Operations (DCO): Ensure that the OPSEC Process is applied to all current and future operations.

9. Area and District Commanders: Designate an Area/District OPSEC Coordinator in writing and provide the name of that responsible person to the Office of Security Policy and Management (DCMS-34).

10. Area and District Security Managers:

    a. Review organizational OPSEC Programs/Plans to ensure compliance with this Manual.

    b. Include OPSEC as an item of interest during unit biennial security evaluations and confirm the following:

        (1) Unit OPSEC Coordinator is appointed in writing

        (2) Unit has an OPSEC plan

        (3) Unit has a Critical Information List

        (4) OPSEC Coordinator has completed an OPSEC Fundamentals course

11. Area/District OPSEC Coordinators:

    a. Complete an OPSEC Program Management course within three months of being assigned coordinator duties. The OPSEC Program Management course may be completed via in-resident training provided by the Interagency Operations Security Support Staff (IOSS) (OPSE-2500).

        (1) The OPSE-2500 course is a USCG Class "C" Training course funded by FORCECOM using AFC-56 funding.

    b. Provide unit OPSEC Coordinator names to attend the OPSE-2500 Program Management and Analysis C-School course to the Office of Security Policy and Management (DCMS-34).

    c. Prepare a compiled Annual Summary Report of OPSEC Activities of units within the Area/District and email it to the Office of Security Policy and Management (DCMS-34) no later than 1 Nov. The format for this report is contained in Enclosure 6.

    d. Compile OPSEC support service requests (Enclosure 7) from subordinate units for external OPSEC services (e.g., training, survey, program development, etc) to the Office of Security Policy and Management (DCMS-34) no later than 1 Sep.

    e. Conduct an annual self-assessment of their OPSEC Program (see enclosure 5).

12. Bases, Districts, Sectors, Area Cutters, Air Stations, Maritime Safety and Security Teams (MSSTs), Tactical Law Enforcement Teams (TACLETs), and Shore Infrastructure Logistics Centers (SILC): Designate a unit OPSEC Coordinator in writing.

13. Unit OPSEC Coordinators:

    a. Ensure compliance with the provisions of this Manual by incorporating sound OPSEC principles into all operational planning and activities to include the development and maintenance of a unit OPSEC plan and unit Critical Information List.

    b. Complete an OPSEC Fundamental course within 3 months of being assigned Unit OPSEC Coordinator duties. The OPSEC Fundamentals course may be completed via online training provided by the IOSS (OPSE-1301 Computer-based training) or through the CDSE website (IO-OP101.16).

    c. Ensure unit compliance with OPSEC Awareness Training annually. The OPSEC Awareness Training can be completed by taking the mandated "A" Security Fundamentals course located on the Coast Guard Learning Management System: https://elearning.uscg.mil/catalog.

    d. Conduct an annual self-assessment of their OPSEC Program (see Enclosure 5).

    e. Provide unit OPSEC Coordinator name to cognizant Area/District OPSEC Coordinator.

    f. Prepare an Annual Summary Report of OPSEC Activities and forward it to the cognizant Area/District OPSEC Coordinator no later than 30 September. The format for this report is contained in Enclosure 6.

    g. Submit requests for external OPSEC support services (e.g., training, survey, program development, etc) to the cognizant Area/District OPSEC Coordinator (see Enclosure 7).

    h. Actively promote (market) the OPSEC concept to the local unit through innovative posters and other information sources, as well as effective training programs.

    i. Conduct random spot checks to involve trash/recycle bin checks to ensure proper disposal of SBI/PII/FOUO information and unobtrusively observe office chatter on phones and in public spaces for any OPSEC concerns. These spot checks are recommended to be conducted at least monthly.

NOTE: It is recommended whenever practical, a member of the operations staff be assigned the OPSEC Coordinator responsibility. This staff member is in the best position to identify Critical Information and to plan and implement OPSEC Countermeasures, in close coordination with the Command Security Officer, Police Chief (where applicable) and other members of the organization's Antiterrorism/Force Protection Working Group.

J. OPSEC PLANNING. OPSEC considerations must be integral to all operational planning**.** Therefore, commanders must ensure that sound OPSEC Principles are incorporated early into the planning and coordination process. Those principles will be codified in a written OPSEC Plan, or OPSEC Annex to an Operational Plan. OPSEC planning is a continuous process. During all phases

of an operation, feedback on the success or failure of OPSEC countermeasures should be evaluated based on each countermeasures' effectiveness, and the OPSEC plan should be modified accordingly. There are two types of OPSEC Plans: (1) Organizational and (2) Activity.

1. Organizational Plans: These plans outline the broad OPSEC Program objectives for the organization. A useful format for Organizational OPSEC Plans are as follows:

   a. References: This Manual, and other OPSEC references as applicable.

   b. Purpose: To establish an OPSEC Program.

   c. Scope: Concise statement of the program.

   d. Policy: Statement of Command Policy on protection of sensitive information.

   e. Process/Procedures: The five-step OPSEC Process.

   f. Responsibilities: Designation of the OPSEC Coordinator and Office of Primary Responsibility.

   g. OPSEC Evaluation: How OPSEC will be evaluated in the organization: (i.e., OPSEC Survey, Command Inspection, and Security Manager's Inspection).

   h. Program Goals: List specific benchmarks for the organizational OPSEC Program, (i.e., establish an OPSEC Working Group, accomplish annual OPSEC Refresher Training, ensure an OPSEC Annex to all Operations Plans are published).

2. Activity Plans: These are the OPSEC Plans that are applicable to individual operations, projects, or activities undertaken by the organization. They may be published as standalone plans or as annexes to the Plans/Orders for a specific operation. The format for such plans should include: Statement of Purpose (Commander's Intent), the five-step OPSEC process; Critical Information, Threat, Vulnerabilities, Risk Assessment and Countermeasures, as well as the communications/control measures and logistics required to implement effective countermeasures.

K. OPSEC TRAINING AND EDUCATION. OPSEC Training and Education is a continuous requirement**.** To facilitate this continuity, USCG OPSEC Training consists of three levels:

1. Introductory Training: This mandatory training is conducted upon entry into the service, or initial civilian employee orientation. It consists of an introduction to basic OPSEC Principles (OPSEC Fundamentals), the broad threat directed against the USCG, and the five-step OPSEC Process.

2. Annual Awareness/ Refresher Training: This mandatory training shall be conducted annually and serves as an OPSEC refresher for all hands. It is conducted by the unit and normally consists, as a minimum, of a review of the current threat for the Area of Operations, insider threat awareness,

a review of the five-step OPSEC Process, and appropriate discussion of the practical application of countermeasures within the organizational operational framework.

3. OPSEC Practitioners Training: This training may take many forms. It is designed for those staff members that are assigned OPSEC Coordinator responsibilities, and or are routinely involved in OPSEC Planning or Program Management. The training is available from the Interagency OPSEC Support Staff (IOSS) as the National Security Agency (NSA) action agency for OPSEC training and education. Programs of instruction include an OPSEC Fundamentals Course, OPSEC Analysis Course, OPSEC Program Management Course, Public Release Decisions Course, and Internet Based Capabilities Course. These courses are offered at the IOSS Training facility, or via a Mobile Training Team (MTT). A full course catalogue may be obtained from the IOSS web site: http://www.ioss.gov.

L. OPSEC EVALUATION. There are several methods to evaluate organizational OPSEC Programs:

1. OPSEC Surveys: An OPSEC survey is a thorough examination of a unit or an operation to determine exploitable vulnerabilities of critical information and to recommend Countermeasures. It is not an inspection; rather it is a fact-finding versus fault-finding operation. It is also a snapshot in time, which is conducted both on-site and off-site by a team of subject matter experts. The survey includes collecting information from a wide range of sources, both directly and indirectly, making observations and interviewing personnel. A USCG unit, through its cognizant District/Area OPSEC Coordinator or Security Manager, can request an OPSEC Survey (see Enclosure 7). All external OPSEC Surveys will be coordinated through DCMS-34. Units should expect to commit personnel for the normal period of the survey. When an OPSEC Survey is completed, a report will be prepared for the requesting unit and will not be distributed without the specific permission of that unit. Lessons learned are encouraged to be shared.

2. Communications Security (COMSEC) Monitoring: COMSEC monitoring provides the means to detect unauthorized disclosures of classified and SBU government information on non-secure telecommunication circuits and systems. Reference L is the controlling directive for COMSEC monitoring of government telecommunication systems. Commandant (CG-65) is the overall program office for CG COMSEC monitoring. Per Reference M, the CYBERCOM Security Operation Center (CSOC) has primary responsibility for reporting and acting on all reported computer-related disclosures. This includes classified, SBU, information contained on the CIL, essential elements of friendly information (EEFI), and PII disclosures. Per Reference K, the Coast Guard Telecommunications System is subject to COMSEC monitoring at all times. The CG uses monitored information to identify trends, vulnerabilities and weaknesses and it is not meant for punitive action. Awareness of active COMSEC monitoring of government telecommunication systems is an essential element of deterrence of such disclosures. In order to keep the program office advised of all incidents, users shall copy Commandant (CG-65) on all CSOC reporting.

3. OPSEC Self Assessment: This is a self-evaluation effort that is conducted by the organization's OPSEC Coordinator on an annual basis. The unit OPSEC activities for a one year period, including training, are reviewed to determine compliance with this Manual and national level

guidelines. A subjective assessment is made to determine the effectiveness of the overall OPSEC effort, and identify areas for improvement (see enclosure 5).

4. Security Manager Evaluations: In accordance with Physical Security Program, COMDTINST M5530.1 (series), District and Area Security Managers (SM) conduct inspections of the security functions for which Command Security Officers (CSO) are responsible. These broad inspections are conducted every two years with the CSO doing a self inspection on the alternate year. SM and CSO inspections will include OPSEC as a functional area for examination. In those cases where the CSO and OPSEC Coordinator are Separate staff functions as recommended herein, the SM or CSO will coordinate the OPSEC portion of the evaluation with the unit OPSEC Coordinator.

M. COMPETING ACTIVITIES.

1. Commanders must consider that a number of potential competing activities, including statutory requirements, exist which can conflict with the fundamental OPSEC goal of protecting information. Examples of potentially conflicting actions include routine press/media releases, foreign military sales, treaty provisions, the Freedom of Information Act and cost-benefit analysis. Each of these legitimate requirements presents some degree of risk for the release of sensitive information. Commanders must exercise extreme caution in determining what information can and should be protected, while satisfying both statutory requirements, and the basic principles of a free and open government. This judgment requires a delicate balance, in which compromises must often be made. Such compromises are inherent in the commander's Risk Management process. In order to preclude potential abuse of the OPSEC Program, commanders will ensure that:

   a. OPSEC Countermeasures implemented are commensurate with the value of the information being protected.

   b. Countermeasures do not restrict higher headquarters from performing their oversight responsibilities relating to fiscal responsibility, waste, fraud and abuse, and compliance with open government statutory requirements.

Note: Questions that arise pertaining to a conflict between OPSEC and statutory requirements should be addressed to the organization's Judge Advocate General (JAG) office.

N. OPSEC RESOURCES.

1. DCMS-34 OPSEC SharePoint Site:

   a. The DCMS-34 SharePoint site is designed to help OPSEC Coordinators develop and enhance their unit's OPSEC Program. The site has applicable OPSEC guidance from DHS and the Coast Guard, as well as templates, samples, and training material covering a wide range of OPSEC topics: http://hqs-spweb10-001:10116/sites/DCMS34/opsec.

b. The DCMS-34 SharePoint is only accessible through the CG One Network (CGOne).

2. Interagency Operations Security Support Staff (IOSS):

a. The IOSS website allows users to order OPSEC awareness products (posters/videos), to enroll in IOSS training courses, and to access to other various OPSEC resources.

b. The mission of the IOSS is to act as a consultant to other U.S. government departments or agencies by providing technical guidance and assistance that will result in self-sufficient OPSEC Programs for the protection of U.S. operations. IOSS staff assesses OPSEC programs, assists in OPSEC program development, conduct surveys and assessments, and provides OPSEC training: https://www.iad.gov/ioss/index.cfm.

3. DCMS-341 Personnel: Unit OPSEC Coordinators shall route all OPSEC concerns through their Area/District OPSEC Coordinators. DCMS-341 personnel are available for OPSEC Program Development and Review, OPSEC Surveys, All Hands training, OPSE-2500 registration (IOSS), and various other OPSEC services (see enclosure 7).

4. Center for Development of Security Excellence (CDSE): Provides a basic working knowledge of Operations Security (OPSEC) and how it applies to Department of Defense (DoD) agencies, components and contractors. The course focuses on the history of OPSEC and the OPSEC process as described in NSDD-298: http://www.cdse.edu/catalog/operations-security.html.

TERMS AND ABBREVIATIONS

1. **Acoustic Intelligence (ACINT):** Intelligence Information derived from the study of acoustical phenomenon.

2. **Classified Information:** Information which has been determined by Executive Order to require protection against unauthorized disclosure, and is marked to indicate the classified status when in documentary form.

3. **Communications Intelligence:** Technical and intelligence information derived from the intercept of foreign communications, by other than the intended recipients of those communications.

4. **Communications Security (COMSEC):** The protection resulting from all measures designed to deny unauthorized persons information of value that might be derived from the possession and study of telecommunications, or to mislead unauthorized persons in their interpretation of the results of such possession and study. Communications Security includes: cryptosecurity, transmission security, emission security, and physical security of communications security materials and information A. Cryptosecurity- The component of communications security that results from the provision of technically sound cryptosystems and their proper use. B. Transmission security- The component of communications security that results from all measures designed to protect transmissions form interception and exploitation by means other than cryptanalysis. C. Emission security- The component of communications security that results from all measures taken to deny unauthorized persons information of value that might be derived from intercept and analysis of compromising emanations form crypto-equipment and telecommunications systems. D. Physical security- The component of communications security that results from all physical measures necessary to safeguard classified equipment, material, and documents form access thereto or observation thereof by unauthorized persons.

5. **Computer Security (COMPUSEC):** The protection resulting from all measures to deny unauthorized access and exploitation of friendly computer systems.

6. **Controlled Unclassified Information (CUI):** A categorical designation that refers to unclassified information that does not meet the standards for National Security Classification under Executive Order 13556, as amended, but is (i) pertinent to the national interests of the United States or to the important interests of entities outside the Federal Government, and (ii) under law or policy requires protection from unauthorized disclosure, special handling safeguards, or prescribed limits on exchange or dissemination.

7. **Countermeasure:** An appropriate and authorized action, such as awareness training or other recommended measure that effectively negates or reduces the risk of an adversary exploiting a vulnerability.

8. **Counterintelligence (CI):** Information gathered and activities conducted to identify, deceive, exploit, disrupt or protect against espionage, or other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, or persons, or their agents, or international terrorist organizations or activities.

9. **Critical Information:** Specific facts about U.S. intentions, capabilities, or activities, vitally needed by adversaries for them to plan and act effectively so as to guarantee failure or unacceptable consequences for U.S. mission accomplishment.

10. **Critical Information List (CIL):** The compilation of information relating to an organization, its organization, missions, and operations that is deemed sufficiently sensitive so as to require a degree of protection, less than actual classification.

11. **Deception:** Those measures taken to mislead an enemy/adversary by manipulation, distortion or falsification of evidence in order to induce a reaction from the adversary which is prejudicial to the adversary's interest.

12. **Essential Secrecy:** The desired end state when denial of critical information to an adversary has been achieved.

13. **Electronic Intelligence (ELINT):** Technical and geo-location intelligence derived from foreign communications transmissions (e.g. radar) by other than nuclear detonations or radioactive sources.

14. **Electronic Security (ELSEC):** Protection resulting from measures designed to deny unauthorized persons information from the interception and analysis of non-communications emissions.

15. **Foreign Intelligence Entities (FIE):** Any known or suspected foreign organization, person, or group (public, private, or governmental) that conducts intelligence activities to acquire US information, block or impair U.S. intelligence collection, influence U.S. policy, or disrupt U.S. systems and programs. This term includes a foreign intelligence and security service [FISS] and international terrorists

16. **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.

17. **Human Intelligence (HUMINT):** A category of intelligence derived from information collected and or provided by human sources.

18. **Imagery Intelligence (IMINT):** Intelligence derived from the exploitation of collection of visual photography, infrared sensors, lasers, electro-optics and radar sensors such as

synthetic aperture radar, wherein images of objects are reproduced optically, electronically on film, electronic display devices, or other media.

19. **Indicator:** Any detectable activity and/or information that when examined alone, or in conjunction with other information, would allow an adversary to obtain critical or sensitive information.

20. **Information Security (INFOSEC):** The protection of information and information systems against unauthorized access or modification of information, whether in storage, processing, or transit, and against denial of service to unauthorized users. Information security includes those measures necessary to detect, document and counter such threats. Information Security is composed of Computer Security (COMPUSEC) and Communications Security (COMSEC).

21. **Insider:** Any person with authorized access to any United States Government resource to include personnel, facilities, information, equipment, networks or systems.

22. **Insider Threat:** The threat that an insider will use their authorized access, wittingly or unwittingly, to do harm to the security of the United States. This threat can include damage to the United States through espionage, terrorism, unauthorized disclosure of information, or through the loss or degradation of departmental resources or capabilities.

23. **Measurement and Signature Intelligence (MASINT):** Technically derived intelligence that detects, locates, tracks, identifies, and describes the unique characteristics of fixed and dynamic target sources. Measurement and signature intelligence capabilities include radar, laser, optical, infrared, acoustic, nuclear radiation, radio frequency, spectroradiometric, and seismic sensing systems, as well as gas, liquid, and solid materials sampling and analysis.

24. **Open Source Intelligence (OSINT):** Information of potential intelligence value that is available to the general public.

25. **Operations Security (OPSEC):** An analytical process used to deny potential adversaries information about capabilities and intentions by identifying, controlling, and protecting generally unclassified evidence of the planning and execution of sensitive activities.

26. **OPSEC Coordinators:** Staff members that are responsible to implement the USCG OPSEC Program within their organization or functional area.

27. **OPSEC Indicators:** Data derived from friendly detectable actions and open-source information that adversaries can interpret and piece together to reach conclusions or estimates of critical or classified information concerning friendly intentions, capabilities, or activities.

28. **OPSEC Infraction:** The failure to execute a security countermeasure established through the application of the OPSEC risk management process, thereby creating an unacceptable level of risk (i.e. increased vulnerability) to items identified on a Critical Information List (CIL).

29. **OPSEC Process:** The analytical five-step, risk based process that includes: Identification of Critical information, Analyzing Threat, Analyzing Vulnerabilities, Assessing Risk, and Applying Countermeasures.

30. **OPSEC Program Manager:** The individual responsible for the overall USCG OPSEC Program at HQ USCG.

31. **OPSEC Survey:** A detailed analysis of all activities associated with a specific operation, project, or program in light of the known collection capabilities of potential adversaries.

32. **OPSEC Working Group (OWG):** A group established by the Department of Homeland Security (DHS) OPSEC Program Manager, consisting of representatives from each DHS organization, to provide a forum for issues relating to OPSEC.

33. **Physical Security (PHYSEC):** The security discipline concerned with the physical measures designed to guard personnel, prevent unauthorized access to an installation, facility, equipment, material and documents, and to prevent espionage, sabotage, damage and theft.

34. **Risk Assessment:** The process of evaluating security risks based on the analysis of threat to and/or vulnerabilities of a system or operation.

35. **Sensitive Information:** Certain information, the release of which could cause harm to a person's privacy or welfare, adversely impact economic or industrial institutions, or compromise programs or operations essential to the safeguarding of our national interests

36. **Signals Intelligence (SIGINT):** A category of intelligence comprising either individually or in combination all Communications Intelligence (COMINT), Electronic Intelligence (ELINT), and Foreign Instrumentation Intelligence, however transmitted.

37. **Signal Security (SIGSEC):** The broad term for the security discipline that includes both communications Security (COMSEC) and Electronic Security (ELSEC).

38. **Telemetry Intelligence (TELINT):** Technical and intelligence information derived from the intercept, processing, and analysis of foreign telemetry. This is a sub-category of Foreign Instrumentation Signals Intelligence.

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

40. **Threat Analysis:** An examination of an adversary's capabilities and intention to exploit vulnerabilities.

41. **Threat Assessment:** An evaluation of the intelligence collection threat to a program or activity.

42. **Trash Intelligence (TRASHINT):** The collection of information, normally unclassified, of potential intelligence value, disposed of by an organization, and subsequently recovered from an organization's refuse receptacles by an adversary. This term has now been expanded to include information gleaned from recycle containers as well. Though not an official government term, it is widely used in DOD counterintelligence operations, and has gained acceptance in private industry as well.

43. **Vulnerability:** 1. The susceptibility of a nation or military force to any action by any means through which its war potential or combat effectiveness may be reduced or its will to fight diminished. 2. The characteristics of a system that cause it to suffer a definite degradation (incapability to perform the designated mission) as a result of having been subjected to a certain level of effects in an unnatural (manmade) hostile environment. 3. In information operations, a weakness in information system security design, procedures, implementation, or internal controls, that could be exploited to gain unauthorized access to information, or an information system.

44. **Vulnerability Analysis:** A process which examines a friendly operation from the perspective of an adversary, who seeks to determine Critical information in time to disrupt or defeat that operation.

45. **Vulnerability Assessment (VA):** A comprehensive examination of the security posture of a facility or installation to determine vulnerabilities.

CRITICAL INFORMATION LIST (CIL)

A. PURPOSE. The purpose of the USCG Critical Information List (CIL) is to facilitate the identification and protection of Coast Guard critical operational information from adversarial exploitation.

1. Our adversaries, whether they are drug or human smugglers, illegal fishermen, domestic or international terrorists, seek to exploit us in any way they can. We must be especially careful not disclose our intentions. By understanding and actively protecting our intentions, capabilities and limitations, we can deny them any advantage.

2. OPSEC considerations must be integral to all operational planning. Therefore, Unit commanders must ensure that sound OPSEC principles are incorporated early into the planning and coordination process. The first step in OPSEC planning is to identify critical information and develop a CIL. Critical information is related to Coast Guard missions and operations and deemed sufficiently sensitive so as to require a degree of protection.

3. The USCG CIL serves as a baseline in developing OPSEC plans for all USCG Units who create, process, transmit or store information identified as mission critical and requiring protection. The items identified on the USCG CIL represent the minimum each unit will include in their CIL. Units should add additional items or specific detailed critical information depending on the mission and/or local circumstances. Depending on the nature and specificity of the information, the unit CIL may require special handling and safeguarding in accordance with References E, F, H, and J listed in this manual.

4. Public disclosure of the USCG CIL is limited by one or more exemptions of the Freedom of information Act (FOIA). Allowing the USCG CIL to be sent to a personal e-mail account constitutes release to the Internet and is not authorized. Chapter 5 of Reference J applies to this CIL - transmission of sensitive government information to personal e-mail accounts is prohibited.

B. DISCUSSION. Due to the constant need to review and update the FOUO Coast Guard Critical Information List, the official CIL is located on the DCMS-34 OPSEC SharePoint Site (http://hqs-spweb10-001:10116/sites/DCMS34/opsec).

COMMON OPSEC INDICATORS

A. PURPOSE. The purpose of this enclosure is to offer a baseline of possible indicators to facilitate OPSEC planning. This enclosure provides a few examples of OPSEC indicators. This is NOT an all-encompassing list as there are many other indicators possible for the wide range of Coast Guard operations and activities.

B. PERSONNEL.

1. Temporary duty (TDY) orders.
2. Conferences.
3. Transportation arrangements.
4. Billeting arrangements.
5. Schedules.
6. Plans of the day.
7. Leave for large groups or entire units.
8. Reserve mobilization.
9. Changes to daily schedules.
10. Emergency recall of personnel on leave and liberty.

C. OPERATIONS, PLANS AND TRAINING.

1. Changes in force protection condition (FPCON).
2. Movement of forces into position for operations.
3. Abnormal dispersions or concentrations of forces.
4. Deviations from routine training.
5. Rehearsals and drills for a particular mission.
6. Exercises and training in particular areas with particular forces.
7. Standard reactions to hostile acts.
8. Standardizing maneuvers or procedures.
9. Changing guards at fixed times.

D. COMMUNICATIONS.

1. Voice and data (telephone, cellular phone, wireless) transmissions between participants in an operation.
2. Changes in message volume (phone calls to secure systems), such as increased radio, e-mail, and telephone traffic.
3. Identification of units, tasks or locations in unsecured transmissions.
4. Increased communications checks between units/organizations.
5. Unnecessary or unusual increase in reporting requirements.
6. Sudden imposition of communications security measures, such as radio silence.

E. INTELLIGENCE, COUNTERINTELLIGENCE, AND SECURITY.

1. Embarking or moving special equipment.
2. Unique or highly visible security to load or guard special munitions or equipment.
3. Adversary radar, sonar or visual detection of friendly units.

4. Friendly unit identifications through communications security violation, physical observation of unit symbols, etc.
5. Trash and recycle bins that contain critical information.

F. LOGISTICS.

1. Package or container labels that show the name of an operation, program or unit designation.
2. Prepositioning equipment or supplies.
3. Special equipment issue.
4. Emissions other than communications.
5. Radar and navigational aids that reveal location or identity.
6. Normal lighting in a blackout area.
7. Operating at unusual speed in water.
8. Loud vehicle or personnel movements.
9. Smoke and other odors.

G. RESEARCH DEVELOPMENT, TEST AND EVALUATION, AND ACQUISTION ACTIVITIES.

1. Solicitations for subcontractors to perform portions of the work.
2. Lists of installations that are involved in particular contracts or projects.
3. Highlighting specific security needs or requirements for portions of a projected contract.
4. Unencrypted emissions during tests and exercises.
5. Public media, particularly technical journals.
6. Deployment of unique units, targets and sensor systems to support tests associated with particular equipment or systems.
7. Unusual or visible security imposed on particular development efforts that highlight their significance.
8. Stereotyped use of location, procedures and sequences of actions when preparing for and executing test activity.
9. Courses of Actions (COA), current and future capabilities

H. INSIDER THREAT.

1. Visits to foreign diplomatic facilities that are unexplained or inconsistent with an individual's official duties.
2. Personnel repeatedly unwilling to comply with rules and regulations, or to cooperate with information security requirements.
3. Repeated security violations.
4. Unauthorized use of another person's account credentials.
5. Unexplained storage of encrypted data.
6. Unauthorized use of multiple user or administrator accounts.

OPSEC COUNTERMEASURES

A. PURPOSE. The purpose of this enclosure is to offer countermeasure examples to help minimize or control vulnerabilities, threats, and the utility of critical information to adversaries (i.e. reduce risk). This is NOT an all-encompassing list. There are many other countermeasures possible for the wide range of possible Coast Guard vulnerabilities.

B. OPERATIONS AND LOGISTICS.

1. Randomize the performance of functions and operational missions. Avoid repetitive or stereotyped tactics and procedures for executing operations or activities in terms of time, place, and event sequencing.
2. Employ force dispositions that conceal the location, identity and command relationships of major units.
3. Conduct support activities in a way that will not reveal intensification of preparations before initiating operations.
4. Operate to minimize the reflective surfaces that units and weapon systems present to radar and sonar.
5. Use darkness to mask deployments or force generation.
6. Approach an objective “out of the sun” to prevent detection.
7. Randomize patrol routes, departure times, speeds, and so forth.
8. Do not set patterns to patrolling activities (start times, locations, number of personnel in a patrol and so forth).
9. Do not use same approach or route into and out of an area repetitively.

C. TECHNICAL.

1. Use radio communications emission control, low probability of intercept techniques, traffic flow security, UHF relay via aircraft, burst transmission technologies, secure phones, landline and couriers.
2. Maintain noise discipline, operate at reduced power, proceed at slow speeds, and turn off selected equipment.
3. Use camouflage, smoke, background noise, added sources of heat or light, paint or weather.
4. Use deceptive radio transmissions.
5. Use decoy radio or emission sites.
6. Follow all security and telecommunications policies for sending unclassified e-mails with sensitive or critical information.

D. ADMINISTRATIVE.

1. Avoid bulletin board plan of the day or planning schedule notices that reveal when events will occur.
2. Conceal budgetary transactions, supply requests and actions and arrangements for services that reveal preparations for activity.
3. Conceal the issuance of orders, the movement of specially qualified personnel to units and the installation of special capabilities.

4. Control trash dumping or other housekeeping functions to conceal the locations and identities of units.
5. Destroy (burn, shred, and so forth) paper to include unclassified information to prevent the inadvertent disposal of classified and sensitive information.
6. Follow normal leave and pass policies to the maximum extent possible before an operation starts in order to preserve an illusion of normalcy.
7. Ensure that personnel discreetly prepare for their family's welfare in their absence and that their families are sensitized to their potential abrupt departure.
8. Randomize security in and around installation/camp to prevent setting pattern or observable routine.
9. Conduct random internal unannounced identity and security inspections.
10. Do not discuss operational or sensitive information in public places.

OPSEC PROGRAM SELF-ASSESSMENT CHECKLIST

Name of OPSEC Coordinator:_____ Date of Self-Inspection:_____

1. Responsibility:	**Yes**	**No**	**NA**
A. Is the organization/unit OPSEC Coordinator appointed in writing? **(REQUIRED)**			
B. Is the OPSEC Coordinator from the operations or plans staff?			
C. Has the name of the OPSEC Coordinator been passed to higher headquarters?			
E. Is the identity of the OPSEC Coordinator posted throughout the unit on bulletin boards and/or electronically?			
F. Are OPSEC contact numbers readily available to unit personnel?			
G. Is the OPSEC Coordinator or POC aware of their responsibilities IAW COMDTINST M5510.24 (series)?			
H. Has the Coordinator completed an OPSEC Fundamentals Course? **(REQUIRED)**			
I. Has the OPSEC Coordinator requested or attended any advanced OPSEC Practitioners Training?			
2. Continuity:	**Yes**	**No**	**NA**
A. Does the OPSEC Coordinator maintain a working/continuity folder?			
B. Are copies of all current OPSEC reference materials on hand, including: COMDTINST M5510.24 (series), DHS Management Directive, and current OPSEC ALCOASTS?			
C. Is there a local instruction (Area, District or Unit) to supplement the Commandant's Instruction? **(REQUIRED)**			
D. Does the continuity file contain copies of: past Self-Assessments, externally conducted OPSEC Assessments/Surveys, results of Security Manager's Inspections relating to OPSEC, annual OPSEC Activities Reports?			
E. Does the continuity file contain a paper record of completion of Security Fundamentals (Mandated "A" Training) and of unit attendance of any OPSEC Refresher Training conducted?			
3. Command Emphasis:	**Yes**	**No**	**NA**
A. Does the Commander/Director actively advocate, support and implement OPSEC Principles in operational planning?			
B. Has the commander/director issued a Command OPSEC Policy Letter to reinforce organizational OPSEC Program objectives?			
C. Is the unit Critical Information List (CIL) reviewed and approved by the commander/director?			
D. Is OPSEC integrated into the Command Information program?			

4. Awareness and Participation:	Yes	No	NA
A. Does the unit/organizational OPSEC Program actively promote individual awareness and participation?			
B. Are OPSEC posters or other graphic materials prominently displayed throughout the unit?			
C. Are OPSEC educational materials available for unit personnel?			
5. Critical Information:	**Yes**	**No**	**NA**
A. Has the unit/organization developed a Critical Information List (CIL)? **(REQUIRED)**			
B. Does the unit CIL consider input from each functional activity?			
C. Is the CIL current, specific, and realistic?			
D. Is the CIL accessible to unit personnel?			
E. Are unit personnel familiar with their functional areas of the CIL?			
F. Is the CIL adequately protected?			
G. Is the CIL updated periodically?			
6. Threat Information:	**Yes**	**No**	**NA**
A. Does the unit maintain current threat data?			
B. Does the OPSEC Coordinator regularly obtain updated Threat data? If so, with whom does he/she coordinate (liaison) to get that information?			
C. Is current Threat information considered (Annex) in the development of Operational Plans, Orders, Exercise Scenarios, RDT&E and Acquisition Programs?			
D. Are current Threat capabilities and intentions correlated with the unit CIL?			
7. Training:	**Yes**	**No**	**NA**
A. Does the unit have an active OPSEC Training program?			
B. Does that training program include an OPSEC orientation for newly assigned personnel?			
C. Does the training program include annual OPSEC refresher training for all assigned personnel? **(REQUIRED)**			
D. Is unit OPSEC training tailored to the unit's mission?			
E. Does unit OPSEC training review the OPSEC Process, the unit's CIL and the indicators of that Critical Information?			
F. Does unit OPSEC training contain a focus on individual responsibility?			
8. Integration:	**Yes**	**No**	**NA**
A. Is the unit OPSEC Program fully integrated with…			
A-1. Information Security (INFOSEC) efforts?			
A-2. Communications Security (COMSEC) efforts?			
A-3. Information Assurance (IA) efforts?			
A-4. Physical Security (PHYSEC) efforts?			

	B. Is the OPSEC Coordinator/POC on distribution for the results of COMSEC Monitoring?			
9. Evaluation and Reporting:		**Yes**	**No**	**NA**
	A. Does the unit have an active OPSEC assessment and reporting effort?			
	B. Has an internal OPSEC Self assessment been made? If so when was the last one conducted? **(Provide date in comments box below)**			
	C. Has an external OPSEC Survey been conducted? If so, when was the last one conducted? **(Provide date in comments box below)**			
	D. Is an annual OPSEC Activities Report prepared and forwarded to higher headquarters? **(REQUIRED)**			
	E. Are lessons learned from self-assessment or external evaluations incorporated into the unit OPSEC Program?			
10. Open Source Information:		**Yes**	**No**	**NA**
	A. Does the unit OPSEC Program adequately consider the risks associated with Open Source Information?			
	B. Is the unit web site periodically "scrubbed" for sensitive information? If so, how often is this done?			
	C. Are command publications i.e. newsletters (official and unofficial), command directives/instructions, daily plans for the day, reviewed for sensitive information?			
	D. Is a periodic check of trash (TRASHINT) and recyclable materials made to screen for sensitive information? How often is this accomplished? **(REQUIRED) (Provide date in comments box below)**			
	E. Is there a process for destruction/disposal of computer disks/CD's that contain sensitive, but unclassified information?			
11. Comments:				

OPSEC ACTIVITIES ANNUAL REPORT
PROCEDURES AND FORMAT

A. PURPOSE. The annual OPSEC status report provides key information on the fundamental management of OPSEC activities across USCG major commands (Area & District) and informs management where program emphasis is necessary.

B. PROCEDURES. A report of annual OPSEC program administration is required per paragraph V.D.3 of DHS MD 11060.1. Coast Guard Units at the Area and District levels will report their OPSEC program status to the DCMS-341 OPSEC Program Manager annually, no later than 30 November. A Separate report will be submitted for each staff office. OPSEC coordinators will use the USCG Annual Operations Security (OPSEC) Status Report to report their annual program status. This report format found on the proceeding pages, is also available on the DCMS-34 SharePoint site.

C. REPORTING CATEGORIES. The major categories of the annual report consist of OPSEC Coordinator; Program Management; Training & Awareness; OPSEC Mission Activities; and Program Review.

1. OPSEC Coordinator: The purpose of this section is to document that, at a minimum, each District and AREA has an OPSEC coordinator formally assigned. “Formally assigned” means that OPSEC coordinators have been named in writing and have completed requisite training.

2. Program Management: The purpose of this section is to document that minimum OPSEC program requirements have been satisfied. Each District and AREA will have an approved OPSEC Plan and conduct a periodic review of that plan. In addition, each District and AREA will have a published CIL as part of their OPSEC Plan.

3. Training and Awareness: The purpose of this section is to document that mandated OPSEC training is accomplished and documented for all assigned personnel.

4. OPSEC Mission Activities: The purpose of this section is to document OPSEC process involvement in operational mission activities.

5. Program Review: The purpose of this section is to provide an opportunity to expand or clarify items in the previous sections. Use this section to highlight significant program accomplishments, best practices or shortfalls.

D. DISPOSITION OF DATA. Data from these reports will be consolidated and provided to the DHS Office of Security, OPSEC Program Office to satisfy the requirement for annual Component OPSEC program reporting.

USCG ANNUAL OPERATIONS SECURITY (OPSEC) STATUS REPORT
AREA & DISTRICT LEVEL

(Calendar Year: 20__)

USCG Unit:
Primary OPSEC Coordinator:
Phone & Email:
Alternate OPSEC Coordinator (If Assigned)**:**
Phone & Email:
Name and signature of person completing this report:

A. OPSEC Coordinator			
ITEM	**Yes**	**No**	**N/A**
1. Has an OPSEC coordinator(s) been appointed in writing?			
2. Does the unit have a signed copy of the appointment letter on file?			
3. Has a copy of the appointment letter been provided to the DCMS-3412 OPSEC Program Manager?			
4. Has the OPSEC Coordinator(s) completed OPSEC Fundamentals training within 30 days of assignment?			
B. Program Management			
1. Have the Unit OPSEC coordinators been scheduled for OPSEC training (OPSE 2500) within 90 days of appointment?			
2. Has the Unit prepared an OPSEC plan?			
a. If yes, has a copy of the Unit's OPSEC plan been provided to your cognizant Area/District OPSEC Coordinator?			
3. Is the Unit's OPSEC Plan reviewed triennially for accuracy and updated as necessary?			
a. If yes, have the Unit's changes been provided to your cognizant Area/District OPSEC Coordinator?			
4. Has the Unit developed a Critical Information List (CIL)?			
5. Have unit personnel have been made aware of the CIL?			

ITEM	Yes	No	N/A
6. Has the OPSEC Coordinator(s) conducted a self-inspection of their Unit's OPSEC program?			
C. Training & Awareness			
1. Are Unit personnel compliant with annual mandated OPSEC training? Number and percentage of personnel trained: 0000 / 00.0 % ***Note: Mandated Training "A" - Security Fundamentals (https://elearning.uscg.mil/catalog/)***			
2. Has the OPSEC Coordinator taken action to address non-compliance with mandated OPSEC training?			
D. OPSEC Mission Activities			
1. Does the Unit OPSEC Coordinator actively engage the command to ensure OPSEC is considered in Unit mission planning? ***Note: Provide examples in Section D.***			
E. Program Overview			
Use this section to expand on items already covered or to highlight your OPSEC program initiatives, projects, successes, or shortfalls not covered in the checklist.			

DCMS-34 OPSEC SUPPORT REQUEST

A. SERVICES OFFERED.

1. Survey- A 3 day staff assistance visit that includes: Command Inbrief/Outbrief, Program Review, All Hands Training, Dumpster Diving, and Personnel Interviews.

2. All Hands Training- A 45 minute briefing covering the 5 step OPSEC process and it's relation to the CG mission; including discussions on the Information Assurance policy, CG vulnerabilities, and countermeasures.

3. OPSEC Program Development/Review- Complete review of unit's OPSEC program. Areas covered include: Program Management, Training, Awareness, Program Effectiveness, Open Source Vulnerability, and Marketing.

4. OPSEC Coordinator Training- For locations that can have multiple OPSEC coordinators meet in a single location for a 1-day OPSEC working group/training session (i.e. multiple stations, cutters, and sectors meet at a Base).

B. REQUEST SUBMISSION.

1. Unit OPSEC Coordinators must coordinate all DCMS-34 OPSEC support through their cognizant Area/District OPSEC Coordinator.

2. Upon Area/District OPSEC Coordinator approval, Unit OPSEC Coordinators can submit a formal request to DCMS-34.

3. The OPSEC Support Request format is available on the DCMS-34 SharePoint site.