Note: January 2023.

This Directive may no longer be current. Please check with the program office responsible for this Directive to determine if there are any updates or if the Directive is no longer in use.

U.S. Department of
Homeland Security

**United States
Coast Guard**

Security Education Training and Awareness (SETA) Program

**COMDTINST M5528.1A
February 2013**

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

Deputy Commandant for Mission
Support
United States Coast Guard

2100 Second Street S.W.
WASHINGTON DC 20593
Staff Symbol: DCMS
Phone: 202-372-4546
Fax: 202-372-4973

COMDTINST M5528.1A
25 February 2013

COMMANDANT INSTRUCTION M5528.1A

Subj: COAST GUARD SECURITY EDUCATION, TRAINING, AND AWARENESS (SETA) PROGRAM

Ref: (a) Department of Homeland Security (DHS) Instruction 121-01-011, Administrative Security Program
(b) Coast Guard Counterintelligence Program, COMDTINST 3850.1
(c) Telecommunication Manual, COMDTINST M2000.3
(d) Guard Security and Information Assurance Manual, COMDTINST M5500.13 (series)
(e) Personnel Security and Suitability Program, COMDTINST M5520.12 (series)
(f) Classified Information Management Program, COMDTINST M5510.23 (series)
(g) Executive Order 13526, Classified National Security Information
(h) Physical Security and Force Protection, COMDTINST, M5530.1 (series)
(i) Operations Security (OPSEC) Program, COMDTINST M5510.24
(j) Department of Homeland Security (DHS) Management Directive Number 11042.1, Safeguarding Sensitive but Unclassified (FOUO) Information
(k) Department of Homeland Security (DHS) Management Directive Number 11056.1, Sensitive Security Information
(l) Coast Guard Industrial Security Program, COMDTINST 5520.13 (series)

1. PURPOSE. This Manual establishes the United States Coast Guard SETA Program. The program is designed to facilitate the implementation of the SETA requirements and standards contained within the full range of security disciplines that comprise the Coast Guard Security Program: Physical Security (PHYSEC), Information Security (INFOSEC), Personnel Security (PERSEC), Operations Security (OPSEC), Industrial Security, and Antiterrorism and Force Protection (AT/FP).

DISTRIBUTION – SDL No. 162

	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							
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		
D	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							
F																			X							
G	X	X	X	X	X																					
H																										

NON STANDARD DISTRIBUTION

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. Intranet release authorized.

3. DIRECTIVES AFFECTED. This manual replaces COMDTINST M5528.1, Security Awareness Training and Education, dated 3 August 1993.

4. BACKGROUND. The overall effectiveness of Coast Guard security is largely dependent on establishing a firm foundation of training and awareness. The SETA Program provides that foundation.

5. CHANGES. Changes will be issued as Commandant's Notices. Time sensitive amendments will be promulgated by ALCOAST, pending their inclusion in the next change to this manual.

6. FORMS/REPORTS. The forms referenced in this Manual are available in USCG Electronic Forms on the Standard Workstation or on the Internet: http://www.uscg.mil/forms/; CGPortal at https://cgportal.uscg.mil/delivery/Satellite/uscg/References; and Intranet at http://cgweb.comdt.uscg.mil/CGForm.

7. RECORDS MANAGEMENT CONSIDERATIONS. This manual has been thoroughly reviewed during the directive clearance process and it has been determined that there are records scheduling requirements, in accordance with Federal Records Act, 44 U.S.C. 3101 et seq., NARA requirements and records created by compliance with the requirements of this manual, will be maintained in accordance and Information and Life Cycle Management Manual, COMDTINST M5212.12 (series).

8. ENVIRONMENTAL ASPECT AND IMPACT CONSIDERATIONS. The potential environmental impacts of this action has been carefully considered and found to be covered by Categorical exclusion 1 e (Figure 2-1 COMDTINST 16475.1E) as it is a guidance document that implements, without substantive change, the applicable Commandant Instruction, procedures, manuals, and other guidance documents. None of the limitation noted in Chapter 2B (2)(b)(2) of COMDTINST 16475.1E exist.

9. DISCLAIMER. This document is intended to provide operational requirements for Coast Guard personnel and is not intended to nor does it impose legally-binding requirements on any party outside the Coast Guard.

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

RECORD OF CHANGES

CHANGE NUMBER	DATE OF CHANGE	DATE ENTERED	CHANGE ENTERED BY

TABLE OF CONTENTS

CHAPTER 1. INTRODUCTION

A. Purpose. This manual establishes the United States Coast Guard Security Education, Training, and Awareness (SETA) Program. The program is designed to facilitate the implementation of the SETA requirements and standards contained within the full range of security disciplines that comprise the Coast Guard Security Program: Physical Security (PHYSEC), Information Security (INFOSEC), Personnel Security (PERSEC), Operations Security (OPSEC), Industrial Security, as well as the interdisciplinary functional areas of Antiterrorism and Force Protection (AT/FP).

B. Scope. This manual outlines the requirements identified in Reference (a) for security training across all security disciplines, to include individual and staff SETA responsibilities. It also recommends the design, development, and implementation guidelines for maintaining an effective state of security awareness throughout the Coast Guard.

C. Objectives. The objective of the Coast Guard SETA Program is twofold:

1. To develop and reinforce a continuous state of security awareness throughout the service.

2. To outline security education requirements for all service members, managers, and professional security staff.

D. Applicability. This manual applies to all U.S. Coast Guard personnel including: service members (active and reserve), auxiliarists, civilian employees and all contractors providing support to USCG activities and operations.

E. Terms and Abbreviations. Enclosure (1)

F. Authorities.

1. Presidential Memorandum, Classified information and Controlled Unclassified Information, May 27, 2009

2. Executive Order (E.O.) 12829, as amended, “National Industrial Security Program”

3. Executive Order (E.O.) 13526, “Classified National Security Information”

4. Executive Order (E.O.) 12968, “Access to Classified Information”

5. Executive Order (E.O.) 13231, “Critical Infrastructure Protection in the Information Age”

6. Presidential Decision Directive/NSC-12

7. Homeland Security Presidential Directive (HSPD) 12 , "Policy for a Common Identification Standard for Federal Employees and Contractors"

8. Homeland Security Presidential Directive (HSPD) 7, "Critical Infrastructure Identification, Priority and Protection"

9. National Security Defense Directive (NSDD) 298, "National OPSEC Program"

10. Public Law 107-347, E-Government Act of 2002, Title III, Federal Information Security Management Act (FISMA) of 2002

11. 32 Code of Federal Regulations (CFR) part 2001 and 2004, "Classified National Security Information Directive No. 1"

G. Responsibilities.

1. Vice Commandant. Assign headquarters staff responsibility for SETA.

2. Subordinate Commanders. Force Readiness Command (FORCECOM) Commander, LANTAREA and PACAREA Commanders, District, Base and Sector Commanders, Commanders of Air Stations, Commanders of Cutters, Commanders of Logistics and Service Centers, and Commanders of Headquarters Units will:

   a. Ensure compliance with this directive.

   b. Assign responsibility for SETA within their Areas of Responsibility (AOR).

   c. Budget for SETA materials and the continuing education of security staff.

   d. Monitor and ensure compliance for mandated SETA training via the Coast Guard Business Intelligence (CGBI) Portal.

3. Superintendant of the Coast Guard Academy and Training Center Commanders.

   a. Ensure required initial security training: OPSEC Awareness, Information Security, and Level 1 AT/FP Training are conducted for entry level recruits, cadets and Officer Candidates.

   b. Ensure AT/FP Level III, OPSEC Awareness, and Threat Awareness Training are incorporated into all Pre-Command, Pre Executive Officer (PCO/PXO), and Prospective Operations Officer (POPS) courses.

   c. Ensure security awareness training is integrated into all officer and non-commissioned officer professional development programs.

4. Assistant Commandant for Human Resources (CG-1).

a. Include applicable security briefings into the personnel in-processing/orientation day schedule.

b. Coordinate security briefing content with DCMS-34, Office of Security Policy and Management.

5. Government and Public Affairs Directorate (CG-092). Integrate security awareness reminders into Command Information Programs.

6. Judge Advocate General of the Coast Guard (CG-094). Ensure Coast Guard compliance with statutory requirements for SETA.

7. Force Readiness Command (FC-T).

a. Determine appropriate performance intervention through thorough analysis as requested and resourced by the appropriate program manager.

b. Manage resourced quotas for C Level Security Training Courses within and external to the Coast Guard to insure baseline and continued professional development of Coast Guard security professionals.

c. Establish standards and certify curricula used for Security Education Classes/Courses, A and C Levels, taught at Coast Guard Training Centers and/or provided by supporting contractors.

8. Counterintelligence Service (CG-CI). Establish standards, conduct training, and document compliance for CI Awareness Training as outlined in Reference (b).

9. Assistant Commandant for C4 and Information Technology (IT), Chief Information Officer (CG-6). Establish standards and document compliance for IT Security Education, Training, and Awareness as outlined in Reference (c) and Reference (d).

10. Office of Security Policy and Management (DCMS - 34).

a. Establish Coast Guard SETA policy and provide management and oversight of the program.

b. Appoint a SETA Program Manager to manage security training and to monitor compliance with Coast Guard SETA Policy.

c. Identify and evaluate SETA materials and methods of instruction for use throughout the Coast Guard.

d. Disseminate SETA best practices.

e. Publish a periodic SETA Newsletter and post on the Intranet. Ensure widest dissemination through Area and District Security Managers.

f. Establish and manage an Intranet based portal to store pertinent CG security data and facilitate collaboration across the CG Security Enterprise.

g. Represent the Coast Guard at SETA panels, forums and meetings with DHS and other government and private entities.

h. Conduct AT/FP Level III Training at Pre-Command/Pre-XO and Prospective Operations Officers (POPS) Courses.

i. Coordinate with the Deputy Directorate for Operations, Joint Staff for Combating Terrorism (J-34) for the CG attendee quotas at AT/FP Level IV Training, and provide support to that training, as required.

j. Manage the Command Security Officer Training Course.

k. Distribute and manage Security Training quotas provided by FC-TRM and course attendance for Coast Guard, DoD, Contract, and other Federal Agency schools.

l. Develop and maintain Annual SETA Mandated Training "A" E-Learning on the CGPortal for all Coast Guard Active Duty, Reserve, and Civilian personnel.

11. <u>Area and District Security Managers</u>.

a. Incorporate both SETA compliance and program effectiveness in inspection checklists.

b. Ensure widest dissemination of DCMS-34 Newsletters throughout their command.

12. <u>Command Security Officers</u>.

a. Serve as the Unit Commander's SETA point of contact.

b. Establish and maintain a SETA program consistent with the SETA practices identified in this manual with the objective of raising security awareness within their command.

c. Establish a SETA self-inspection program and evaluate organizational SETA Programs in preparation for higher headquarters evaluations.

d. Ensure SETA is properly administered at local orientation briefings for all incoming personnel.

e. Conduct SETA for their assigned unit and/or command.

f. Include SETA as an area of interest during annual self-evaluations.

g. Ensure widest dissemination of DCMS-34 Newsletters throughout their command.

h. Liaison with the unit training officer to ensure security specific training is being updated and maintained within TMT as need or applicable. Note: only applies if training is done in-person.

i. Liaison with the unit Training Officer to make available unit training records to the Cognizant Security Manager, as required.

j. Submit training requests to Cognizant Security Manager for unit member attendance to “C” schools.

13. Individual. Security Awareness is an individual responsibility for all Coast Guard personnel, employees and contractors. Policy and physical or electronic barriers alone cannot protect Coast Guard resources. These measures must be effectively coupled with a work force that fully understands security policies and accepts responsibility for compliance with those standards. The most effective measure of protection against exploitation is a workforce that is aware and engaged.

CHAPTER 2. LEVELS OF LEARNING

A. Interdisciplinary Relationship. The overall effectiveness of the multi-discipline Coast Guard Security Program is largely dependent on establishing a firm foundation for the range of technical competencies, both individual and managerial, that contribute to that program. The SETA Program provides that foundation.

When considered in aggregate, Security Education, Training, and Awareness form an educational continuum that builds from baseline knowledge to core competency level through professional certification. The SETA program must remain adaptive and provide for continual reinforcement.

B. Key Components. The Coast Guard SETA Program consists of three components that are progressive in nature and mutually supporting: Security Education, Security Training and Security Awareness. They are defined as follows:

1. Security Education. Security Education integrates security skills and competencies into a common body of knowledge, policies or doctrine to be studied by security professionals i.e. OPSEC Program Managers course, Command Security Officers course, AT/FP Training Level II, etc.

2. Security Training. Security Training produces relevant security skills and competencies to support job performance: OPSEC Process, Classification and Marking, IT Security Practices, etc. There are three types of training utilized within the SETA Program framework:

   a. Mandatory Training. Security training required by statute, directive, or other regulatory guidance.

   b. Specialized Training. Security training specifically designed to facilitate sound security practices in individual job performance.

   c. Professional Training. Technical or Certification training for the professional security staff.

3. Security Awareness. Security Awareness focuses individual attention on security needs or concerns and promotes positive security consciousness. It facilitates positive changes in behavior or reinforces good security practices: OPSEC Awareness, Foreign Travel Briefing, CI Awareness Briefing, etc.

C. Audience. Each component of the Coast Guard SETA program is focused on a different target audience. Security Education (Professional) is generally limited to those with specific security responsibilities, the security professionals: Security Managers, Command Security Officers, AT/FP Officers, etc. Security Training has a broad based audience, but can be tailored based on individual duties and mission, i.e., Commanders, Managers and Technical Staff. Security Awareness is focused on the entire service population and is universally applicable to all echelons of the organization.

D. Knowledge and Skills. Each type of security training, including awareness, has an accompanying set of knowledge or skills in connection with the target audience. That knowledge or skill set can range from simple identification of individual security responsibilities to technical competency in a particular security discipline – a Subject Matter Expert (SME).

CHAPTER 3 POLICY AND PROCEDURES

A. General.

1. The SETA program includes, but is not limited to the development and presentation of the following:

   a. Initial Security and Orientation Briefing. An initial security briefing is provided to all Coast Guard personnel who have met the standards for access to classified information. Prior to being granted access to classified information, individuals receive a comprehensive briefing to inform them of the basic security policies, principles, practices, and criminal, civil, and administrative penalties. At that time, individuals execute a Standard Form 312(SF-312), “Classified Information Nondisclosure Agreement.” The signed SF-312 is witnessed by the individual conducting the briefing or another Office of Security person assisting with the briefing, and submitted to the individual’s Component Personnel Security division for filing in their permanent personnel security file. An individual is only required to sign a SF-312 once unless they have been debriefed, or their clearance has been administratively withdrawn; in which case they receive another briefing and a new SF-312 is signed prior to receiving access.

   b. Annual Security Fundamentals Mandated Training. All Coast Guard Military and Federal employees, to include contractor employees, consultants, and detailed personnel are required to complete Security Fundamentals training within the first 30 days of assignment. The Security Fundamentals Mandated “A” Training Course is located on the Learning Management System (LMS) Portal. The SETA course fulfils annual refresher training requirements for OPSEC, INFOSEC, and AT/FP Level 1. The Security Fundamentals course also addresses the threat and techniques employed by foreign intelligence activities attempting to obtain classified information, and advises personnel of penalties for engaging in espionage activities.

   c. Original Classification Authority (OCA) Training. OCAs receive training in proper classification and declassification with an emphasis on the avoidance of over-classification. At a minimum, the training covers classification standards, classification levels, classification authority, classification categories, duration of classification, identification and markings, classification prohibitions and limitations, sanctions, classification challenges, security classification guides, and information sharing. This training is provided prior to the individual originally classifying information and at least once each calendar year thereafter. Original classification authorities who do not receive this mandatory training at least once within a calendar year will have their classification authority suspended until such training has taken place, unless a temporary waiver has been approved. OCAs sign an acknowledgement at the completion of the training session.

d. Derivative Classifier Training. Persons who may apply derivative classification markings, regardless of media, receive training and are certified prior to taking any derivative classification actions. Training includes the proper application of the derivative classification principles, the avoidance of over-classification and, at a minimum, the principles of derivative classification, classification levels, duration of classification, identification and markings, classification prohibitions and limitations, sanctions, classification challenges, security classification guides, and information sharing. In addition to this preparatory training, derivative classifiers are required to receive such training at least once every two years. Derivative classifiers who do not receive this mandatory training at least once every two years have their authority to apply derivative classification markings suspended until they have received the proper training unless a temporary waiver is granted.

e. Termination Briefings. Individuals receive termination briefings to inform them of their continuing security responsibilities after their access authorizations are terminated. A termination briefing is accomplished on the individual's last day of employment, the last day the individual possesses an access authorization, or the day it becomes known that the individual no longer requires access to classified information. The Command Security Officer (CSO) or other individuals that the CSO delegates will conduct the termination briefing via the SF-312. Once the individual has been debriefed and signed the acknowledgement statement of the SF-312, this record becomes part of the individual's permanent personnel security file.

f. Other Specialized Training. Classification management specialists, security managers, security specialists, declassification authorities, and all other personnel whose duties significantly involve the creation or handling of classified information receive more detailed additional training no later than six months after assumption of duties that require this specialized training.

Training topics may include, but are not limited to: overview of DHS safeguards and security disciplines, including personnel security, information security, physical security local access control procedures and escort requirements, protection of government property, locks and containers, risk management reporting and notification requirements, legal and administrative sanctions imposed for incurring a security infraction or committing a violation, construction security, SCIF construction, and/or foreign intelligence service threats to sensitive and classified information.

B. Documentation Requirements.

1. Records are maintained for four years to identify all individuals who have received briefings by type and date of briefing. Record keeping systems provide an audit trail. Statistics should pertain to total population and numbers that have received security briefings.

2. The Coast Guard Business Intelligence (CGBI) portal is the primary tool CG leadership uses to track training completion.

TERMS AND ABBREVIATIONS

Antiterrorism (AT)
Defensive measures used to reduce the vulnerability of individuals and property to terrorist acts to include limited response and containment by military and civilian security forces.

Antiterrorism Awareness
The basic knowledge of the terrorist threat and the measures to reduce personal vulnerability to threat attacks.

Antiterrorism Officer (ATO)
A commander's principle staff officer advisor for AT/FP matters.

Area of Responsibility (AOR)
The geographic area for which a commander has jurisdiction or responsibility, and in which he/she has authority to plan and conduct operations.

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.

Coast Guard Business Intelligence (CGBI) Portal
CGBI is a decision support system that provides users with a web-based toolset containing standardized Coast Guard enterprise data and provides access to Enterprise, Unit, Personal information; Reports; and Cubes. CGBI turns Coast Guard data into information by which knowledge is gained for wise decision-making.

Command Security Officer (CSO)
The CSO is that individual in whom the Commanding Officer (CO) has vested staff responsibility for all matters relating to the security of an installation, organization, or cutter.

Communications Security (COMSEC)
The protection resulting from all measures designed to deny unauthorized persons information 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. COMSEC includes Crypto-security, Transmission Security, Emissions Security, and Physical Security of communications security materials and information.

Controlled Unclassified Information (CUI)
The Umbrella term used for a framework that calls for the consolidation and standardization of many designations, definitions, and standards used throughout the government to identify information as sensitive but unclassified.

Counterintelligence (CI)
Information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, 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.

Force Protection (FP)
The security program developed to protect Coast Guard personnel, civilian employees, contractors, family members, facilities and equipment, in all locations and situations against all hazards.

Information Assurance (IA)
Operations that protect and defend information and information systems by ensuring confidentiality, integrity, availability, authenticity, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

Information Security (INFOSEC)
Those security measures applied to the protection of information (electronic or printed) from unauthorized disclosure which could reasonably be expected to cause damage to national security.

Industrial Security
Procedures and processes for insuring civilian contractors doing business with the U.S. Government follow rules for accessing and safeguarding classified material entrusted to them.

Information System Security Officer (ISSO)
Individual responsible for the implementation and maintenance of security for an Information System.

Information Technology (IT)
Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by an organization. The term Information Technology includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services) and related resources.

Mandated Training
The Mandated Training Program includes the coordination, planning, development, maintenance, delivery, and tracking of all federally and organizationally mandated training requirement. This program falls under the authority of Force Readiness Command Training Division (FC-T). Policy guiding mandated training requirements and its associated content remains the responsibility of the program office. There are two distinct types of Mandated Training requirements in the Coast Guard: MT Category "A" and MT Category "B".

Operations Security (OPSEC)
A systematic analytical process to identify critical information and analyze friendly actions attendant to operations and other activities to: identify those actions that can be observed by an adversary, determine indicators that might be interpreted or pieced together to derive critical information of use to an adversary, and the selection of methods/procedures to control, eliminate or mitigate the risks for hostile exploitation.

Personnel Security (PERSEC)
The security discipline that covers all aspects of security relating to personnel including: screening (Background Investigation and Adjudication) to determine suitability for and retention of employment, and granting and retaining specific access to classified/sensitive information.

Physical Security (PHYSEC)
The security discipline that employs physical and procedural measures to detect, deter, and defend personnel, property, equipment, facilities and information against espionage, terrorism, sabotage, damage, misuse, theft and other criminal acts.

Security
Precautions taken by an individual, activity, installation, etc. to guard against and mitigate an occurrence of crime, attack, sabotage, espionage or other hostile act.

Security Awareness
The state of mind members of an organization possess regarding the importance of the protection of physical and information assets of an organization.

Security Manager (SM)
The USCG Headquarters, Area, or District Command-level staff officer who has responsibility for security planning and management.

Security Education
That portion of the Security Education Continuum that integrates security skills and competencies into a common body of knowledge, policies or doctrine studied by security professionals.

Security Management
A broad field of management pertaining to asset management, Physical Security, and

human resource safety functions.

Security Training
That portion of the Security Education Continuum that produces relevant security skills and competencies for those members requiring such knowledge to effectively perform their managerial or technical duties.

Sensitive But Unclassified Information (SBU)
Information that is not classified for national security reasons, but that warrants/requires administrative control and protection from public or other unauthorized disclosure for other reasons.

Staff Assistance Visit (SAV)
Coast Guard Headquarters on-site support program wherein a team of Subject Matter Experts (SME) assist installation security managers with their security planning needs.

Terrorism
The calculated use of violence or threat of violence to inculcate fear; intended to coerce or to intimidate governments or societies in the pursuit of goals that are generally political, ideological, or religious.

Vulnerability Assessment (VA)
The process through which the commander determines the susceptibility to attack and the broad range of physical threats to the security of an installation/activity and its personnel, and which provides a basis for determining AT Measures that can protect personnel and assets from a terrorist attack. A VA may be either a self-assessment or externally conducted. External assessment of a Coast Guard installation, facility, activity or cutter’s ability to deter or respond to a terrorist incident administered by the Coast Guard Office of Security Management.

REQUIRED SECURITY TRAINING

Training	Audience	Content	Frequency	OPR / Location
Access Briefing	Employees Granted Access (Cleared Employees)	Responsibilities for Safeguarding Classified and SBU Information – Classification Levels, Classification Authority, Cover Sheets, Marking, Declassification, Storage, Transmission, Reporting Violations	Prior To Granting Access Non Disclosure Form SF -312 Required	Personnel / Inprocessing Location
Security Fundamentals Mandated Training (Includes updated versions)	All assigned personnel – Military, Civilian, Contractors	Fulfils annual training requirement for: OPSEC INFOSEC AT/FP Level I	Within 30 days of inprocessing date and annually thereafter	DCMS-341 / CG Portal Learning Management System
* SETA Refresher Briefing	All Employees	INFOSEC OPSEC AT/FP Level 1	Annually	DCMS-341 / CG Portal Learning Management System Or Individual, or All Hands Training Sessions
OPSE 2500 Course	OPSEC Coordinators	OPSEC Analysis & Program Management	Within 90 Days of Assignment	DCMS-341, IOSS Schedule at ioss.gov
CSO Course	Newly assigned CSO's	PERSEC INFOSEC PHYSEC AT/FP Industrial Security OPSEC SETA Security Resourcing	Upon assignment of CSO duties. Contact cognizant security manager for quota	DCMS-341 / Security Center, Chesapeake, VA
AT/FP Level III	Prospective Operations Officers, Executive Officers & Commanders	AT/FP Planning	Prior To Assumption of Duties	CG Academy

AT/FP Level IV	O-6's & Above or Civilian Equivalent	AT/FP Policy Making	As Soon As Practical After Assignment	Joint Staff J-34 & DCMS-3412 (quota management)
Derivate Classification and Marking	Employees designated as Derivative Classification Authorities	Derivative classification application and marking	Initial and Biennial	DCMS-3412
Arrival Briefing for Incoming Unit Personnel	All newly assigned personnel to any Unit	Personnel Security Information Security Loss Prevention Operations Security Industrial Security Program	Within 30 days after arrival to Unit	Command Security Officer/Unit

* Refresher Briefing Presentations may be scheduled individually i.e., INFOSEC, OPSEC and AT/FP or combined in a single training session. All Hands gatherings offer an excellent opportunity to complete annual security training requirements. This type of training must be documented and recorded in CGBI.

SAMPLE TRAINING PLAN TEMPLATE

PURPOSE: This plan outlines the responsibilities, goals and objectives for accomplishment of Security Awareness, Training, and Education (SETA) for Unit X during Calendar year 20XX. It includes both Generally Mandated Training and Specialized Training.

REFERENCES: List all references applicable to training being conducted.

GOALS:

- To ensure a continuous state of Security Awareness for all unit members.
- To maintain or enhance service member proficiency in those security skills required for successful job performance.

OBJECTIVES:

- Attain 100% attendance of unit personnel for all Generally Mandated (Annual) Security Training.
- Ensure appropriate skill certification for all personnel who have specialized security duties/responsibilities.
- Reduce the number of security incidents resultant from lack of training.

Goals versus Objectives

Goals are broad in scope and tend toward the abstract. Objectives are narrower in focus and therefore more concrete. It is difficult to measure Goals alone. Objectives are more measureable as they form the steps to reach a Goal.

SCHEDULE: The following format is a useful design for tracking requirements, and scheduling Security Training

Subject/Frequency	Reference	Audience	Objective	Method	Responsibility	Evaluation
AT/FP Level 1 (Arrival)	COMDTINST M5530.1C	All Personnel	AT Awareness	CD, Brief Packet or On-line	DCMS-341	On-line quiz
Information Assurance (Annual)	COMDTINST M5500.13B	All IT System Users	IT Security Awareness	On-line	CG-6	On-line Quiz
OPSEC Refresher (Annual)	COMDTINST M5510.24	All Personnel	OPSEC Awareness	On-line and/or Classroom	OPSEC Coordinator	On- line, or in class Quiz

CSO Training (As soon as Practical after Appt)	All Security Instructions	Newly Appointed CSO	Certification (Formal POI)	Classroom Lecture and PE (5 days)	DCMS-34 Contractor Provided	Written Exams
OPSEC Program Managers Course (Within 90 Day s of Appt)	COMDTINST M5510.24	Newly Appointed OPSEC Coordinators	Certification (Formal)	Through IOSS	DCMS-34	Written Exam

RESOURCE REQUIREMENTS: The purpose of this section is to quantify the resources expended or needed to adequately administer SETA for a Unit. This section may be optional and/or modified to fit location specific needs.

Method of Instruction is the critical element that defines resources required to present security training. By the far the most resource intensive method of providing security training at a unit is the Lecture Method conducted in a classroom environment by a "live" instructor. This method requires: Appropriate scheduling (Time Allocation) notice, an appointed instructor, lesson plan, adequate classroom space, appropriate audio-visual equipment and training aids, and the mass assembly of personnel to be trained. By contrast, the least resource intensive (and most flexible) method of instruction is web based training.

COST:

Resource	Cost
Staff: Instructor Prep and Contact (Hours)	$$$
Contracting Support: Class/ Course Development/Teaching	$$$
Facilities: Classroom, AV Equipment, Student Materials	$$$
Training Aids: Printing (Student Workbooks, Pamphlets), Manufacture/Procurement Office Supplies	$$$
Media: Web Page, Video/CD Production	$$$
Travel and Per Diem: For personnel to attend training classes	$$$

SAMPLE SECURITY EDUCATION, TRAINING AND AWARENESS PROGRAM CHECKLIST

UNIT: ____ **DATE:** _________________

NAME: ________________________ **SIGNATURE:** ____________________________

ITEM	YES	NO	NA
1. Has a Unit Training Officer TO) been appointed?			
1.1. Is there an appointment letter?			
2. Are all applicable SETA regulatory documents available?			
2.1. DHS Instruction 121-01-001?			
2.2. COMDTINST M5528.1?			
2.3. ALCOASTs (Expire after one year)			
3. Are all personnel completing the mandated annual SETA training requirement?			
4. Does the unit Training Officer maintain training records on unit personnel?			
4.1. Are training records maintained and updated in the Training Management Tool?			
5. Does the unit Training Officer monitor the Mandated Training schedule on the CG Learning Management System?			
6. Does the unit Command Security Officer submit Training Requests to the Cognizant Security Manager for unit member attendance to "A" and "C" schools?			
7. Does the organization have security awareness program? 7.1. Are security awareness posters visible in working areas? 7.2. Are periodic security reminders/tips provided to the workforce to remind and motivate them? 7.3. Are security awareness briefings being provided based on local incidents or security related conditions?			
8. Are the DCMS-34 SETA and Defender Newsletter disseminated throughout the unit?			

Sample Arrival Briefing for Incoming Unit Personnel

Introduction

Welcome, and a special congratulations on your new assignment. Your job makes you a member of a very special team comprised of military and civilian personnel who are engaged in work that impacts the defense of our great nation.

In performing your job, you will be dealing (at a minimum) with unclassified sensitive information. You may also be working with information which has been classified in the interest of our national security - that is, information which is CONFIDENTIAL, SECRET, OR TOP SECRET. Security must become a vital part of your daily routine and always in your forethought. It is essential you know and understand the requirements for protecting government assets, i.e., classified information, property and personnel.

As mentioned before, you are part of a team; in some areas of your life, you have learned how important teamwork is to the final outcome of any event. Every individual must do their part if the team is to be successful. The Coast Guard has established a security program to protect government assets and prevent our adversaries from gaining access to sensitive and critical information. However, no matter how comprehensive the program may be, the key ingredient is people. You and your coworkers will ultimately determine the success of our established procedures. Your daily security vigilance helps us keep our national security advantage and protect the freedoms we all enjoy so much.

NOTE: At this time, inform the individual of security points of contact at the time; e.g., Command Security Officer (CSO), OPSEC Coordinator, Classified Material Control Officer (CMCO), Area and District Security Manager, Unit Information Systems Security Officer (ISSO), etc. Advise them of other information specific to the unit, e.g., where security regulations can be located, where and how to report security incidents, etc.

Personnel Security (Reference (e))

Personnel Security ensures that all individuals working within the U.S. Coast Guard are suitable for employment/service, being reliable, trustworthy and have an unquestionable loyalty to the United States. Prior to reporting to work, unless you transferred from a Coast Guard unit or other government agency, a background investigation was conducted on you by the Office of Personnel Management to determine your suitability for employment with the Coast Guard, and to determine your eligibility for a security clearance (if required). Not every employee will require a security clearance. A security clearance is driven by position and does not follow a person from job to job. For example, a person with a security clearance at one unit may transfer to another unit and not be issued a clearance, or may be granted a clearance at a level higher or lower than the one previously held. It all depends on the needs of the position. Remember, all individuals who have been granted a security clearance must complete a Standard Form 312 (SF-312).

Questionable information collected during the investigation must be clarified and may require further investigation. The information obtained must be evaluated and a common sense determination made taking into consideration all available information. Questionable factors include criminal conduct, alcohol abuse, drug abuse, financial irresponsibility, and falsification of information provided in interviews or on employment forms, or may include other factors that would cast doubt in an individual's responsibility, loyalty, reliability or trustworthiness.

Evaluation of your character and activities does not end after the initial investigation. We have a program that requires a continuing evaluation of your eligibility to hold a security clearance. Your actions can affect your ability to retain a security clearance, and possibly your position. We have learned that one of the greatest threats to our security comes from our own carelessness and complacency.

Any employee, who occupies a position of trust or has access to classified information, has a responsibility to report changes or incidents that may impact their clearance. Such things may include: 1) Marriage to or cohabitation of a foreign born, non-U.S. Citizen; 2) Any derogatory information (financial problems to include bankruptcies, wage garnishments, liens; 3) Arrests regardless of whether or not you were charged; 4) Alcohol or Drug abuse; 5) Illegal involvement with controlled dangerous substances, to include the abuse of prescription drugs or dangerous inhalants; 6) Foreign travel- personal or official business; 7) Substantial Unofficial Foreign Contact; and, 8) Loss or Compromise of National Security Information.

Remember, it takes your cooperation to make this continuous evaluation program work. You have a responsibility to report to your CSO any questionable information that indicates an individual no longer meets the security standards for eligibility to hold a security clearance. You may feel a little uncomfortable about reporting a coworker, but keep in mind the importance of security interests, as well as national security interests, and the good of the entire country. If that person is compromising Coast Guard security, it affects not only the whole U.S. security program, but potentially you and your family as well.

<u>Information Security</u> (Reference (f))

The guidance in Reference (g) prescribes a uniform system for safeguarding national security information. Classified information is official government information that requires protection against unauthorized disclosure in the interest of national security. Unauthorized disclosure occurs when someone who is not authorized by the government to have access to classified information does get access, either accidentally or intentionally.

Access to classified information is permitted only to persons who possess an appropriate security clearance and have an official need-to-know. Your position may or may not require access to classified information. If it does, further information will be provided to you during an “access briefing”. If your position does not require access to classified information, this section is provided in case you inadvertently discover unprotected classified material. You will be able to identify classified information by its markings and properly safeguard it.

There are three categories of classified information that require specified protective measures; the unauthorized disclosure of this information will result in a degree of damage to the national security:

CONFIDENTIAL - The unauthorized disclosure of this information could reasonably be expected to cause "damage" to our national security.

SECRET - The unauthorized disclosure of this information could reasonably be expected to cause "serious damage" to our national security.

TOP SECRET - The unauthorized disclosure of this information could reasonably be expected to cause "exceptionally grave damage" to our national security.

All documents containing classified information will be marked in a prescribed manner to indicate the classification assigned and the degree and duration of protection required. Classification levels will be conspicuously marked or stamped at the top and bottom of all pages. Paragraphs, subjects and titles will be individually marked with parenthetical symbols (TS), (S), or (C). The face of the document will also include "Classified by" and "Declassify on" lines to identify classification sources and declassification and downgrading instructions.

Classified material will be stored in approved secure areas, in GSA approved security containers or under the direct observation of authorized personnel. If by chance, you discover classified material unprotected, i.e., in an incoming mail box, in a copier machine, on top of a file cabinet, on a desk, etc., you have an immediate responsibility to protect the material from further risk and report the incident to your Command Security Officer (CSO). If you cannot both protect the information and report the incident, have someone else make the report while you continue to protect the information.

If you are approached by anyone seeking unauthorized access (i.e., not cleared and/or need-to-know) to classified or sensitive information, immediately report it to your CSO. It is no secret that dedicated foreign intelligence services are working in this country to gain valuable information. Compromised classified information could severely damage America's national security; we must all work together to prevent this from happening.

Loss Prevention (Reference (h))

Care must be taken to ensure that adequate safeguards are established to protect government property from loss or theft. Items considered being highly susceptible to loss or theft, to include, calculators, small office machines, laptop computers, desk clocks, postage stamps, etc. Government funds, controlled medical substances, arms, ammunition and explosives, sensitive forms such as unissued identification cards, purchase orders, and credit cards are also highly susceptible to loss or theft. Careless handling of these items encourage thievery or contributes to their inadvertent loss.

Concern is not only focused on the external threat of criminal activity; it is specifically directed toward the internal threat: theft and pilferage by those who have authorized access. Inattention to physical security practices and disregard for property control and accountability foster an environment of loss.

You are responsible to immediately report to your CSO any missing, lost or stolen government property. Timely reporting increases the possibility that property will be recovered. Reporting losses provides a measure of effectiveness for internal controls, stimulates reviews of inventory and accountability procedures, and reflects both strengths and weaknesses in the security program.

You can support the loss prevention effort by observing the following precautions:

1. Lock up all small items at the close of business.
2. Do not leave money or other valuables in desk drawers.
3. Keep your purse or wallet with you at all times.
4. Make sure coat/clothing racks are well within controlled spaces, not close to exterior doors or open hallways.
5. Require all unknown persons who enter your space to identify themselves. Verify their reason for being there if you are not sure.
6. Report missing, lost or stolen government property, including identification badges and keys.
7. If you observe any suspicious persons or activities in buildings, parking areas, etc., immediately report it to your CSO.

Operations Security (Reference (i))

Operations Security (OPSEC) is 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. The purpose of OPSEC is to enhance operational effectiveness. OPSEC differs from traditional security in that it does not have a fixed set of rules that must be applied. You can imagine all the critical information about the Coast Guard mission as pieces of a jigsaw puzzle. Due to their classification, many of these pieces are protected by security programs such as Information Security. However, much of this critical information is unclassified (Reference (j), or specific to maritime security (Reference (k), and still requires protection. This is where OPSEC comes in. OPSEC enhances operational effectiveness and compliments other security disciplines by protecting the unclassified, critical information that when put together by the adversary, will bring about serious mission degradation or failure.

The OPSEC process is divided into five steps:

1. **Identify the critical information that requires protection.** If this information fell into the adversaries hands, it could bring about serious mission degradation or failure. Examples include personnel rosters, operational mission plans, capabilities or limitations, patrol schedules, and budget information.
2. **Analyze the threat.** A threat is an adversary with the intent and capability to target our critical information. Determine the individuals or groups that represent a threat to our mission – intent and capability must exist.
3. **Analyze the vulnerabilities.** Vulnerability is a weakness that provides an adversary an opportunity to exploit our critical information and bring about mission failure. Think like the adversary and view your organization from their perspective.
4. **Assess the risk.** Risk is the measure of the probability an adversary will be able to compromise your critical information while factoring the impact on your mission if they are successful. Commanders must determine how much risk is acceptable – cost vs. benefit.
5. **Apply countermeasures.** By applying countermeasures, you reduce the risk factors. Countermeasures control or hide indicators and reduce the adversary's ability to exploit our vulnerabilities. Countermeasures may include encrypting sensitive e-mails, shredding documents, avoiding discussing sensitive details on unsecured communications.

How can you apply OPSEC?

As a member of the Coast Guard, it is imperative that you practice good OPSEC in your day-to-day activities. OPSEC is not a process only done at the highest levels, it starts with you. Here are just a few countermeasures that that you can utilize everyday:

1. Properly shred documents containing Personally Identifiable Information (PII), For Official Use Only (FOUO), or any other identified unit critical information.
2. Think before you post! Use caution when posting information such as photos, deployment dates, or any other sensitive work-related information on Social Networking Sites.
3. Use encryption when transmitting critical information via radios, cellular phones, and email.

There are adversaries, such as international spies, terrorists, identity thieves, and sophisticated criminal organizations that want to gain access to our information for their benefit. The use of basic OPSEC principles can ensure that they do not succeed in their illicit intentions. Your understanding and consistent application of OPSEC helps to ensure the success of the Coast Guard mission.

So remember, always "THINK OPSEC!"

Conclusion

Our mission is to establish an awareness and mindset of effective practices on the part of all employees and to ensure compliance with government policies and procedures designed to protect classified information, government property and all personnel. We are here to help you. Here's how you can help us:

1. Understand your individual security responsibilities.
2. Make security a daily habit.
3. Ask if you have any questions, or need help.

Security depends on your cooperation and personal awareness. You are charged to take an active part in protecting The Coast Guard’s vital mission assets, now and in the future.

Industrial Security Program (Reference (l))

This briefing is for government personnel involved with classified contracts, or involved with contractor personnel. The briefing is located on the DCMS-34 SharePoint site at: http://hqsms-spweb-001:116/sites/DCMS34/infosec/default.aspx