DEPARTMENT OF THE NAVY
OFFICE OF THE SECRETARY
1000 NAVY PENTAGON
WASHINGTON DC 20350·1000

SECNAVINST 5510.36B
DUSN
12 Jul 2019

SECNAV INSTRUCTION 5510.36B

From: Secretary of the Navy

Subj: DEPARTMENT OF THE NAVY INFORMATION SECURITY PROGRAM

Ref: See enclosure (1)

Encl: (1) References
(2) Responsibilities
(3) Department of the Navy Information Security Program Overview
(4) Classification Management
(5) Alternative Compensatory Control Measures
(6) Violations of This Instruction
(7) Records Management
(8) Forms and Reports

1. Purpose. Per the authority in reference (a), this instruction updates policy and responsibilities for Classified National Security Information (CNSI) and Controlled Unclassified Information (CUI) within an overarching Department of the Navy (DON) Information Security Program (ISP), pursuant to references (b) through (f); establishes uniform ISP policies and procedures per references (b) through (f); complies with the intent of references (b) and (d) to observe the democratic principles of openness and the free flow of information, as well as to enforce protective measures for safeguarding information critical to national security; incorporates policies and procedures established by other executive branch agencies and supplements volumes 1 through 4 of reference (f), where needed. When applying guidance of this instruction, the user must consult the appropriate volume of reference (f) to ensure proper application of DON and Department of Defense (DoD) ISP standards.

2. Cancellation. SECNAVINST 5510.36A, SECNAV M-5510.36, DUSN (P) ltr 5510 Ser DUSN (P)/006 of 2 Feb 18, and DUSN (P) ltr 5510 Ser DUSN (P)/009 of 31 Aug 16.

3. Definitions. For DoD definitions for the Information, Personnel, Physical, Special Access, and Industrial Security

Programs, see reference (g). Reference (g) can be obtained by accessing the Deputy Under Secretary of the Navy (DUSN) Security Directorate Microsoft SharePoint Portal.

4. Applicability. This instruction applies to the Offices of the Secretary of the Navy (SECNAV), the Chief of Naval Operations (CNO), the Commandant of the Marine Corps (CMC), and all U.S. Navy (USN) and U.S. Marine Corps (USMC) installations, commands, activities, field offices, and all other organizational entities within the DON. It does not alter or supersede the existing authorities delegated to the Director, DON Special Access Program (SAP) Central Office (DON SAPCO) for SAP, per references (h) through (l), or those delegated to the USMC Director of Intelligence (DIRINT) and the Director of Naval Intelligence (DNI) as Heads of the Intelligence Community Elements (HICE) by the Director of National Intelligence as delineated in reference (m).

5. Policy. It is DON policy that:

a. The DUSN is appointed as the DON Senior Agency Official (SAO) for the DON ISP, including SAO responsibilities pursuant to reference (b), and is delegated Top Secret (TS) Original Classification Authority (OCA).

b. The Deputy CNO for Information Warfare, Office of the CNO is designated as the USN HICE for Sensitive Compartmented Information (SCI) as defined in references (a), (f), and (n).

c. The DIRINT is designated as the USMC HICE for SCI as defined in references (a), (f), and (n).

d. The Director, DON SAPCO is responsible for the execution, management, oversight, administration, security, information systems and networks, information assurance, and records management for SAPs under the responsibility of the DON, per references (j) through (l).

e. All personnel of the DON are personally and individually responsible for properly creating/marking, safeguarding, transmitting, and destroying classified information and CUI under their custody and control, per volumes 1 through 4 of reference (f).

f. All officials within the DON who hold command, management, or supervisory positions have specific, non-delegable responsibility for the quality and effectiveness of implementation and management of the DON ISP within their areas of responsibility.

g. National security information will be classified, safeguarded, and declassified per references (b), (c), (f), and (g). CUI will be identified and safeguarded consistent with the requirements of references (d) through (f).

h. Classified information released to industry will be safeguarded, per reference (o).

i. Security requirements and responsibilities for protecting classified information and CUI from Unauthorized Disclosure (UD) will be emphasized in DON Component training programs, pursuant to references (b) through (f).

j. Before being approved for public release, all DoD information will be reviewed pursuant to references (f) and (o) through (r) and other applicable policies including reference (s).

k. Safeguarding requirements and incident response measures addressing willful, negligent, and inadvertent mishandling of classified information, to include on Information Systems, must be implemented across DON, per reference (t).

l. Necessary resources are committed to effectively implement the DON ISP.

m. Management takes prompt and appropriate action in cases of compromise or UD of CNSI and CUI. Such actions shall focus on correcting or eliminating the conditions that caused or brought about the incident.

n. Commanders/Directors are allowed to submit waivers and exceptions through the chain-of-command to the DON SAO when situations arise that require deviation from the standards of this instruction or any of its implementing directives.

o. All personnel with access to classified information systems that are capable of processing North Atlantic Treaty

Organization (NATO) classified information must be briefed on their responsibilities for protecting NATO information and acknowledge in writing the receipt of the NATO briefing.

p. All personnel who are authorized access to classified information systems must complete derivative classification training initially and annually thereafter.

q. To use the current holder of the General Services Administration (GSA) contract for overnight delivery of information for the Executive Branch when the requirement exists for overnight delivery to a DoD Component within the U.S. and its territories. The use of external (street side) collection boxes is prohibited.

r. Volume 2 of reference (f) is the DON authoritative source for marking CNSI. Documents marked per previous guidance or the Information Security Oversight Office (ISOO) Marking Guide do not need to be re-marked. All newly created documents must carry compliant markings per this volume.

s. Volume 4 of reference (f) is the DON authoritative source for marking CUI. CUI will be marked as “For Official Use Only” (FOUO) until DoD publishes new guidance. CUI marked FOUO will be protected per the guidelines of this volume.

t. All persons (i.e., military, civilian, and contractor) must possess a valid and appropriate security clearance, signed a Standard Form (SF) 312, “Classified Information Nondisclosure Agreement,” and a valid need-to-know prior to being granted access to CNSI.

u. Visitors to a DON facility who require access to, or where disclosure of, classified information may occur during the visit will have their identity, security clearance and access level, and need-to-know verified prior to the visit. Unannounced visitors will not be allowed entry to a facility where access to, or where disclosure of, classified information may occur until their identity, security clearance and access level, and need-to-know are verified.

v. The DON SAO, CNO, or CMC may authorize personnel under their authority to remove secret and confidential information from their designated working areas for work at home provided

authority has been granted, per volume 3 of reference (f). The CNO or CMC may further delegate this authority to the heads of Echelon I and II activities. No further delegation is authorized.

6. Responsibilities. See enclosure (2).

7. DON ISP Overview. The purpose of the DON ISP is to ensure classified and controlled CUI is properly created, safeguarded, transmitted, and destroyed (see enclosure (3)).

8. Classification Management. For more information on DON Classification Management, see enclosure (4).

9. Alternative Compensatory Control Measures (ACCM). For information on ACCM, see enclosure (5).

10. Violations of this Instruction. For information on possible disciplinary action and criminal penalties, see enclosure (6).

11. Records Management. See enclosure (7).

12. Forms and Reports. See enclosure (8).

THOMAS B. MODLY
Under Secretary of the Navy

Distribution:
Electronic only, via Department of the Navy Issuance website https://www.secnav.navy.mil/doni/.

REFERENCES

(a) DoD Instruction 5200.01 of 21 April 2016
(b) E.O. 13526
(c) 32 CFR 2001
(d) E.O. 13556
(e) 32 CFR 2002
(f) DoDM 5200.01 volumes 1-4, DoD Information Security Program of 24 February 2012
(g) PDUSD memo, DoD Security Lexicon of 13 June 2013
(h) DoD Directive 5205.07 of 1 July 2010
(i) DoD Instruction 5205.11 of 6 February 2013
(j) SECNAVINST S5460.3H
(k) SECNAVINST 5460.4
(l) SECNAVINST 5430.7R
(m) DoD Directive 5200.43 of 1 October 2012
(n) DoDM 5105.21 volumes 1-3, Sensitive Compartmented Information (SCI) Administrative Security Manual of 19 October 2012
(o) DoD Instruction 5220.22 of 18 March 2011
(p) DoD Directive 5230.09 of 22 August 2008
(q) DoD Instruction 5400.04 of 17 March 2009
(r) DoD Instruction 5230.29 of 13 August 2014
(s) DoD Directive 5122.05 of 7 August 2017
(t) Deputy Secretary of Defense memo, Unauthorized Disclosures of Classified Information or Controlled Unclassified Information on DoD Information Systems of 14 August 2014
(u) SECNAVINST 5500.36
(v) SECNAV memo, Delegation of Declassification Authority for the Department of the Navy Declassification Program of 20 September 2018
(w) Department of the Navy Declassification Guide of 3 December 2018
(x) SECNAVINST 5430.107
(y) DoD Instruction 8500.01 of 14 March 2014
(z) SECNAVINST 5239.3C
(aa) EKMS-1E, Electronic Key Management System (EKMS) Policy and Procedures for Navy Tiers 2 & 3 of 7 June 2017
(ab) SECNAVINST 2201.1
(ac) SECNAVINST 5211.5E
(ad) ICD 704 of 1 October 2008
(ae) JAGINST 5800.7F

(af) SECNAV memo, Delegation of Authority to Grant Waivers and Exceptions to Department of the Navy Information Security Program Policies and Procedures of 15 November 2016
(ag) SECNAV memo, Department of the Navy Security Executive of 25 April 2013
(ah) DoDM 5200.45, Instructions for Developing Security Classification Guides of 2 April 2013
(ai) SECNAVINST 5000.34F
(aj) SECNAV WASHINGTON DC 051800Z Jan 16 (ALNAV 001/16)
(ak) SECNAV M-5214.1

RESPONSIBILITIES

1. SECNAV

a. Approves all DON TS OCA. This authority is not delegable;

b. Approves the removal of TS classified information for work at home, in the absence of the SAO.

2. DUSN. The DUSN, under the authority, direction, and control of the SECNAV:

a. Serves as the DON SAO for both classified and CUI and executes the duties identified in volumes 1 and 4 of reference (f), “Senior Agency Officials;”

b. Reviews and approves/denies waivers and exceptions to this instruction and any of its implementing directives. When necessary, forward the waiver/exception to the Director of Security, Office of the Deputy Under Secretary of Defense, Intelligence and Security (DUSD (I&S));

c. Approves all DON secret OCAs. This authority is not delegable. Submits TS OCA requests to SECNAV;

d. Reviews and approves/denies all classified conferences not held in a cleared government or contractor facility (e.g., hotel, university, etc.). This authority is not delegable;

e. Serves as an impartial official for reviewing formal challenges to classification of DON information. May convene an impartial panel of OCAs to assist with the review;

f. Convenes an impartial panel of OCAs to address any appeals to formal classification challenges of DON information. Different OCAs will be selected if a panel was initially used;

g. Refers formal challenges involving Restricted Data information to the Department of Energy and Formerly Restricted Data to the Deputy Assistant Secretary of Defense, Nuclear Matters;

h. Submits waivers involving marking of classified information to the DUSD (I&S) for submission to the Director, ISOO;

i. Approves removal of TS classified information for work at home;

j. Should consider whether the workforce needs to be reminded of actions to be or not to be taken by DON personnel in response to widely known public disclosures;

k. Maintains a world-wide available government-only private unclassified but secure web presence that provides information related to the DON Security Programs;

l. Designates a CUI program manager to help oversee the DON's entire CUI planning and implementation program, including necessary training.

3. Senior Director for Security and Intelligence. The Senior Director for Security and Intelligence, DUSN Security and Intelligence (S&I) Directorate is responsible for the development of policy and an integrated strategic framework for the management, integration, oversight, and assessment of the DON Security Enterprise and provides staff support for the DUSN functions and responsibilities described in reference (u)

a. Develops guidance as necessary for implementation of the DON ISP;

b. Provides oversight to the DON ISP to assess the effectiveness and efficiency of the DON's ability to create, protect, and destroy classified and CUI;

c. Ensures prompt and appropriate response to any request, appeal, challenge, complaint, or suggestion arising out of implementation of this instruction or any of its implementing directives;

d. Receives information, allegations, or complaints regarding over-classification or incorrect classification within the DON and, as needed, provide guidance to personnel on proper classification;

e. Processes ACCM requests to establish or terminate to the senior agency office for approval. Forwards the written notification within 30 days to the Director of Security, Office of the Under Secretary of Defense for Intelligence (OUSD (I)) or the Director, International Security Programs, Defense Technology Security Administration, Office of the Under Secretary of Defense for Policy (OUSD (P)), as appropriate;

f. Processes annual reports to the SAO and ensures copies are furnished to OUSD (I) and ISOO, as required;

g. Validates OCAs, annually;

h. Coordinates and cooperates with other protection program equities to achieve a harmonized and cohesive ISP within the DON;

i. Processes OCA requests to the SECNAV or SAO, as required;

j. Manages the security directorate web presence ensuring timely accurate information is made available to DON activities;

k. Provides policy and technical support to the Services;

l. Serves as the focal point for Defense Technical Information Center (DTIC) on all DON Security Classification Guide (SCG) inquiries;

m. Serves as the program management office to help oversee the DON’s entire CNSI and CUI planning and implementation programs, including necessary training.

4. Department of the Navy/Administrative Assistant (DON/AA). Per the authorities granted in reference (v), DON/AA is responsible for the implementation and oversight of DON automatic, systematic, and mandatory declassification reviews, including the update and issuance of reference (w). The DON/AA Directives and Records Management Division (DRMD) is the program office that executes DON/AA responsibilities pursuant to this directive as follows:

a. Provides adequate funding and resources to implement the declassification program;

b. Consults with the SAO to determine the declassification action to be taken when a function was dispersed to more than one activity, the inheriting activity(ies) cannot be determined, or the functions have ceased to exist;

c. Develops and issues declassification guidance to facilitate effective review and declassification of information classified under both current and previous CNSI Executive Orders.;

d. Manages the systematic and automatic declassification program in accordance with volume 1 of reference (f);

e. Develops processes for responding to Mandatory Declassification Reviews. Refer to volume 1, “Mandatory Declassification Review” of reference (f) for additional guidance;

f. Is not authorized to declassify cryptological, Restricted Data, Formerly Restricted Data, Naval Nuclear Propulsion Information, SCI, SAP information originated by another department or agency, or Foreign Government Information (FGI) without the prior consent of the originating entity. Refer these documents to the appropriate agency or foreign government for further declassification consideration.

5. Director, Naval Criminal Investigative Service (DIRNCIS). The DIRNCIS is the senior official for criminal investigations and counterintelligence (CI) within the DON. DIRNCIS is the senior official within the DON for terrorism investigations and related operations designed to identify, detect, neutralize, or prevent terrorist planning and activities, and provides antiterrorism expertise and services to DON activities. NCIS initiates, conducts, and directs criminal, CI, terrorism, and related investigations and operations as deemed appropriate, and conducts the full range of CI activities. Additionally, the DIRNCIS is the sole liaison with the Federal Bureau of Investigation on DON security matters, per reference (x).

6. Chief of Information (CHINFO). The CHINFO is the SECNAV’s direct representative for public affairs. CHINFO is delegated the responsibility for coordinating, planning, implementing, and assessing public affair policies and programs of the DON.

7. Director, Navy International Programs Office (NIPO). The Director, NIPO is responsible to the Assistant Secretary of the Navy (Research, Development and Acquisition) (ASN (RD&A)) for:

a. Implementing policies and managing DON participation in international efforts (e.g., Foreign Military Sales and International Agreements) concerning ASN (RD&A).

b. NIPO is responsible for reference (u).

c. Making technology security and foreign disclosure determinations for disclosure of classified and CUI to foreign governments and organizations in compliance with DON and national disclosure policy.

d. Managing personnel exchange programs with foreign governments.

8. DON CIO. The DON CIO is responsible for DON policies and implementation of the DoD cybersecurity program to include the protection of classified information and CUI on DON Information Technology (IT) systems under reference (y). The DON CIO issues reference (z), develops DON-wide Information Management (IM)/IT/Information Risk Management policy, standards, and guidance, and aligns and integrates IM/IT programs across the USN and USMC. The DON CIO is also responsible for policy and oversight of Communication Security (COMSEC), per references (aa) and (ab), and is the DON’s senior military component official for privacy and civil liberties, per reference (ac).

9. CNO and CMC. The CNO and CMC:

a. Approves removal of secret and confidential classified information for work at home for their respective services. This may be delegated to the heads of Echelon I and II commands. No further delegation is authorized;

b. Submits waivers and exceptions to this instruction and any of its implementing directives to the SAO;

c. Submits TS and secret OCA requests to the SAO;

d. Establishes procedures to accommodate visits to their service facilities involving access to, or disclosure of,

classified information and CUI. Refer to volume 3, “Visits” of reference (f) for additional guidance;

e. Submits requests to the SAO for classified meetings and conferences, or classified sessions thereof, that are held at a location other than a cleared U.S. government facility or a U.S. contractor facility that has an appropriate facility security clearance, and as required, secure storage capability to the SAO for approval;

f. Submits Service endorsements on requests to use ACCM for classified information over which they have cognizance to the SAO;

g. Reports confirmed security incidents to the SAO when incidents have or may have significant consequences or the fact of the incident may become public;

h. Manages the Service’s SCG Program, to include issuance of SCG Identification (ID) numbers for all new or revised SCGs in accordance with enclosure (4);

i. Coordinates with the DTIC for SCG retrieval;

j. Encourages classification challenges and establishes procedures for processing formal challenges to DON classified information received from within and from outside their Services in accordance with enclosure (4) of volume 1 of reference (f).

10. Commander, U.S. Fleet Cyber Command (FCC). The Commander, FCC as the USN’s Service Cryptologic Component commander to the National Security Agency/Central Security Service, is responsible for the security program for all Cryptologic field sites as well as Cryptologic and IT personnel, regardless of assignment, per reference (ad).

11. Commander, Naval Communications Security Material System (NCMS). The Commander, NCMS administers the DON COMSEC program as the service authority and serves as the central office of records for all NCMS accounts and COMSEC material throughout the DON, U.S. Coast Guard, and national COMSEC community as required per reference (y).

12. Heads of DON Activities. The heads of DON activities are responsible for overall management, functioning, and effectiveness of the activity's ISP. Authority delegated by this instruction to the head of an activity may be further delegated unless specifically prohibited in reference (g).

a. Execute the duties and responsibilities in volume 1, "Heads of DoD Activities" of reference (f).

b. Submit waivers and exceptions to this instruction and any of its implementing directives through the chain-of-command to the CNO and CMC, for approval. Refer to volume 3, "Waivers and Exceptions" of reference (f) for additional guidance.

c. Determine if TS Control Officers (TSCO) are required to facilitate appropriate control of collateral TS material where there is a need (e.g., accountability of Sigma material). Collateral TS material entering SCI Facilities (SCIF) and SAP Facilities (SAPF) will be processed in accordance with SCI and SAP directives.

d. Determine if other security management roles are necessary for management of the activity ISP in accordance with volume 1, "Other Security Management Roles" of reference (f).

e. Ensure contractors used in security administration are prohibited from performing certain critical, closely associated roles which are inherently governmental, or otherwise exempt functions and activities that cannot or should not be performed by a contractor in accordance with volume 1, "Use of Contractors in Security Administration" of reference (f).

f. Prohibit the use of foreign nationals in security administration in accordance with volume 1, "Use of Foreign Nationals in Security Administration" of reference (f).

g. Ensure all assigned personnel have a valid and appropriate security clearance, have executed an appropriate non-disclosure agreement, and have a valid need-to-know before allowing access to classified information.

h. Ensure all persons with access to classified information systems (e.g., Secret Internet Protocol Router Network (SIPRNet), collateral TS networks, etc.) receive the NATO

briefing and responsibilities for safeguarding NATO classified information, and acknowledge receipt of the brief in writing:

(1) Mass briefing sign-in rosters are not sufficient and may not serve as written acknowledgement of the brief.

(2) For Joint Worldwide Intelligence Communications System (JWICS) access requirements, consult the activity's Special Security Officer (SSO), and follow DNI policy requirements.

i. Ensure classified information and CUI are protected in accordance with this instruction, volumes 1 through 4 of reference (f), and any of its implementing policies.

j. Ensure prompt and appropriate management action is taken in cases of compromise, UD, or loss of classified information or CUI. Report any violation of this instruction, or one of its implementing directives, that results in negligence or willful disclosures of classified information or CUI, as determined by a security inquiry (Preliminary Inquiry (PI)) or investigation (command investigation) in the Joint Personnel Adjudication System (JPAS), or its successor system. Refer to volume 1, "Corrective Actions and Sanctions" of reference (f) and sections 0203 and 0209 of reference (ae) for more information.

k. Submit request for OCA in accordance with enclosure (4) of this instruction, through established organizational channels to the SAO.

l. Not take retribution against any individual for questioning a classification or making an informal or formal challenge to a classification.

m. Submit requests for waivers involving marking of classified information through the chain-of-command to the SAO. Refer to volume 2, "Waivers Involving Marking of Classified Information" of reference (f).

n. Establish a system of security checks at the close of each duty and/or business day where classified information is used is stored securely. Refer to volume 3, "End of Day Security Checks" of reference (f) for documenting the checks. Automated means may be used in place of SF 701, "Activity

Security Checklist" and SF 702, "Security Container Checksheet" (e.g., alarm logs, swipe access logs, etc.).

o. Develop emergency plans to protect, remove, or destroy classified material in case of fire, natural disaster, civil disturbance, terrorist activities, or enemy action to minimize the risk of compromise, and for the recovery of classified information. Refer to volume 3, "Emergency Plans" of reference (f) for additional details. An "Emergency Plan Template" located at the DUSN Security Directorate Microsoft SharePoint Portal may be used.

p. Approve all equipment used to reproduce classified information in writing, and post the approval notice in a conspicuous place where all users can see. In addition, ensure the use of equipment for such reproduction, including controls comply with the standards in volume 3, "Reproduction of Classified Material" of reference (f).

q. Develop activity security procedures to appropriately safeguard information that may retain all or part of information contained in copiers, facsimile machines, computers, and other IT equipment and peripherals, display systems, and electronic typewriters. Refer to volume 3, "Equipment Used for Processing Classified Information" of reference (f).

r. Approve classified meetings or conferences, or classified sessions thereof, that take place in an appropriately cleared U.S. government facility or U.S. contractor facility that has an appropriate facility security clearance and, as required, secure storage capability. Ensure the approval includes the appointment of an activity security manager and the additional requirements and events are conducted in accordance with volume 3, "Classified Meetings and Conferences" of reference (f).

s. Conduct and evaluate risk assessments to determine whether installation of an intrusion detection system is warranted or whether other supplemental controls are sufficient. As a minimum, the risk assessment/analysis shall contain the minimum criteria identified in volume 3, "Risk Assessments" of reference (f).

t. When special circumstances exist, may authorize the use of key operated locks for storing bulky material containing secret and confidential information. The authorization must be in writing and must explain the special circumstances and administrative procedures for control and accounting of keys and locks, outlined in volume 3, “Bulky Material” of reference (f). The keys shall be protected at the level of the classified bulky material.

u. Establish procedures to ensure that hand-carrying of classified material is minimized to the greatest extent possible and does not pose unacceptable risk to the information. Additional guidance is provided in volume 3, “Escort, Courier, or Hand-Carry of Classified Information” of reference (f).

v. Serve as the responsible official by providing a written statement to each individual who is authorized to escort, courier, or hand-carry classified material. Refer to volume 3, “Escort, Courier, or Hand-Carry Authorization” of reference (f) for additional details.

w. Advise their chain-of-command of compromises occurring within their area of security responsibility or involving assigned personnel. If the head of the activity does not have security cognizance over the incident, ensure the incident is reported to the appropriate authority to include forwarding to DUSN (S&I) Directorate, if necessary.

x. Notify appropriate authorities when a security incident reveals information suggestive of a criminal or CI nature is discovered and cease all actions pending coordination with appropriate authorities as outlined in volume 3, “Security Inquiries and Investigations” of reference (f).

y. Immediately notify the OCA if a PI or command investigation determines a loss or compromise has occurred. In addition, notify the SAO through the chain-of-command.

z. Appoint an individual to lead PIs into security incidents to determine the facts and circumstances of the incident in writing. Ensure the appointed individual characterizes the incident as an infraction or a violation. Do not appoint the activity security manager as a PI official. Ensure the official appointed is not involved in the incident.

A “Preliminary Inquiry Convening Order Template” is available at the DUSN Security Directorate Microsoft SharePoint Portal.

aa. Appoint investigating officials in writing, to conduct a command investigation into classified security incidents when the circumstances of an incident require a more detailed inquiry, additional information is needed, or where the head of the activity is contemplating punitive actions. Refer to volume 3, “Security Inquiries and Investigations” of reference (f) for additional guidance and restrictions on appointing a command investigation official.

ab. Take prompt action to resolve deficiencies identified in security incident reports by PI and command investigation officials. Refer to volume 3, “Results of Inquiries and Investigations” of reference (f) for additional details.

ac. Determine if a debriefing is warranted following unauthorized access to classified information. Refer to volume 3, “Debriefing in case of Unauthorized Access” of reference (f) for general guidelines.

ad. Ensure ACCM information, documents, and material are properly:

(1) Safeguarded in accordance with the OCA instructions and volume 3, “Alternative Compensatory Control Measures (ACCM)” of reference (f).

(2) Marked in accordance with volume 2, “Other Dissemination Control Markings: Alternative Compensatory Control Measures (ACCM)” of reference (f).

ae. At a minimum, designate one day per calendar year as a “clean out” day to reduce the amount of the classified and CUI on hand.

13. DON Activity Security Managers. DON Activity Security Managers shall execute the duties in enclosures (2), “Activity Security Manager,” and (3), “Activity Security Management” of volume 1 of reference (f) and shall:

a. Ensure all assigned personnel have a valid and appropriate security clearance, have executed an appropriate

non-disclosure agreement, and have a valid need-to-know before allowing access to classified information. Refer to volume 1, "Access to Classified Information" of reference (f) for more information.

b. Ensure all persons with access to classified information systems (e.g., SIPRNet, collateral TS networks, etc.) receive the NATO briefing and responsibilities for safeguarding NATO classified information, and acknowledge receipt of the brief in writing:

(1) Mass briefing sign-in rosters are not sufficient and may not serve as written acknowledgement of the brief.

(2) For JWICS access requirements, consult the activity's SSO and follow DNI policy requirements.

c. Ensure classified information and CUI is protected in accordance with this instruction, volumes 1 through 4 of reference (f), and any of its implementing policies.

d. Ensure prompt and appropriate management action is taken in cases of compromise, UD, or loss of classified information or CUI. Report any violation of this instruction, or one of its implementing directives, that results in negligence or willful disclosures of classified information or CUI, as determined by a PI or command investigation in JPAS, or its successor system. Refer to volume 1, "Corrective Actions and Sanctions" of reference (f) and sections 0203 and 0209 of reference (ae) for more information.

e. Ensure all OCAs receive training and certify in writing they have received training, before exercising their authority and annually thereafter on the fundamentals of proper security classification and declassification. Emphasis should be made on over-classification, duration of classification, and compilation of information in electronic formats (e.g., databases, spreadsheets) that lead to new aggregations making the information vulnerable to data mining and other data correlations. OCAs shall receive training that covers:

(1) The limitations of their authority;

(2) The sanctions that may be imposed;

(3) OCA duties and responsibilities, as required by volume 3, “OCA Training” of reference (f).

f. Maintain all OCA delegation letters or SECNAV list of OCAs for any positions within their organization, and OCA training certifications. Provide this information when requested by appropriate authorities (e.g., SAO, USD (I), ISOO, etc.).

g. Review all OCA SCGs to ensure they are properly marked and formatted prior to requesting an SCG number from the Service’s DON SCG Program Manager.

h. Assist all DON personnel with submitting tentative classification information to an OCA, when requested.

i. Ensure all organization personnel, prior to accessing a classified Information System (IS), receive derivative classification training as specified in volume 1, “Derivative Classification, Responsibilities of Derivative Classifiers, and Procedures for Derivative Classification” and volume 3, “Initial Orientation” of reference (f) and annually thereafter.

j. Assist personnel (i.e., military, civilian, and contractor) with making informal and formal classification challenges when they believe information is improperly or unnecessarily classified and communicate that belief to the OCA or activity security manager assigned to the OCA.

(1) Prior to submitting the challenge, attempt to validate if the information is properly classified according to SCG or other document transmitting classification guidance.

(2) Encourage personnel to submit an informal challenge before resorting to formal challenge.

(3) Process informal and formal challenges in accordance with volume 1, “Challenges to Classification” of reference (f) through the chain-of-command to the OCA.

(4) In addition to the OCA and/or OCA’s activity security manager, submit copies of all formal challenges to the SAO through the appropriate chain-of-command.

(5) Do not take retribution against any individual for questioning a classification or making of an informal or formal challenge to a classification.

k. Direct personnel outside the DON to enclosure (4) of this instruction and the Service-specific requirements.

l. Sample derivatively classified documents generated by the organization to ensure the documents/materials are marked in accordance with volume 2, “Marking Principles” of reference (f). Figures 1 through 58 of volume 2 are examples of marking most types of derivate classified documents and material. Figure 4 of volume 2 is an example of a derivatively classified document.

m. Sample classified files, folders, and similar groups of documents, and IT systems to ensure they are marked in accordance with volume 2, “Coversheets and Classification Labels” of reference (f).

n. Sample records to validate end of day security checks are conducted and properly documented for the activity.

o. Conduct risk assessments, as needed, to facilitate security–in-depth determinations and to aid in identification and selection of supplemental controls that may need to be implemented. Refer volume 3, “Risk Assessment” of reference (f) for a list of the minimum criteria used in risk assessments.

p. Complete management and oversight training on topics identified in volume 3, “Management and Oversight Training” of reference (f). This may be accomplished by completion of the Navy Security Manager’s Course, online and/or in-residence DoD security specialist or information security management courses, or completion and maintenance of the security fundamentals professional certification under the DoD Security, Professional, Education, and Development Program.

q. Advise their chain-of-command of compromises occurring within their area of security responsibility or involving assigned personnel. If the activity security manager does not have security cognizance over the incident, ensure the incident is reported to the appropriate authority to include up channeling to DUSN Security Directorate, if necessary.

r. Ensure certain types of classified information or specific circumstances are addressed using unique handling or consideration of additional reporting, as defined in volume 3, "Special Circumstances" of reference (f).

s. Notify the head of the activity when a security incident reveals information suggestive of a criminal or CI nature is discovered and cease all actions pending coordination with appropriate authorities as outlined in volume 3, "Security Inquiries and Investigations" of reference (f).

t. Immediately notify the head of the activity if a PI official or command investigating official determines the security incident has resulted in a loss or compromise. If directed by the head of the activity, notify the OCA, and through the chain-of-command, notify the SAO.

u. When authorized, appoint an individual to lead inquiries into security incidents to determine the facts and circumstances of the incident and to characterize the incident as an infraction or a violation. Ensure the official appointed is not involved in the incident.

v. Consult with the head of the activity and take prompt action to resolve identified deficiencies identified by PI and command investigation officials' security incident reports. Refer to volume 3, "Results of Inquiries and Investigations" of reference (f) for additional details.

w. Address IT issues in accordance with volume 3, "IT Issues for the Security Manager" of reference (f).

14. TSCO. When designated, a TSCO shall execute the duties in volume 1, TSCO, enclosure (2) and TSCO, enclosure (3), of reference (f).

15. The HICE, Deputy CNO for Information Warfare/DNI (N2/N6) and DIRINT shall execute the duties identified in volume 1, "Senior Intelligence Officials" of reference (f), and references (n) and (ad) for their respective service.

16. The Director, DON SAPCO shall execute responsibilities for SAP, per references (h) through (l).

17. IS Security Officials (ISSO) (e.g., authorizing official, IS Security Manager, and IS Security Officer). When designated, an ISSO shall execute the duties in volume 1, "Information Systems Security Officials" of reference (f). In addition:

a. Work closely with activity security managers at all levels, security specialists, and DUSN Security Directorate to ensure classified information and CUI are properly protected when data and/or information resides on IT and IS, and networks managed and controlled by the DON CIO.

b. If not already done, notify the activity security management when data spills occur and assist the security manager as required. Security personnel have the overall lead for addressing such events, while IT and/or cybersecurity staff have overall responsibility for the operation of the networks and systems.

18. Military Commanders of Military Operations. Military commanders are authorized to modify the provisions of this instruction and any of its implementing guidance pertaining to accountability, dissemination, transmission, and storage of classified and controlled unclassified material and information as necessary to meet local conditions encountered during military operations. Refer to volume 1 of reference (f) for a definition of Military Operations.

19. All DON personnel (i.e., military or civilian) who hold command, management, or supervisory positions shall:

a. Have specific, non-delegable responsibility for the quality and effectiveness of implementation and management of the DON ISP within their areas of responsibility.

b. Ensure classified information and CUI are protected at all times by following the guidance in this instruction and volumes 1 through 3 of reference (f) for the protection of classified information and volume 4 of reference (f) for the protection of CUI.

c. Submit Waivers and Exceptions to this instruction and any of its implementing directives through their service chain-of-command to the SAO. Refer to reference (af), and volume 3,

"Waivers and Exceptions" of reference (f) for additional guidance.

d. Ensure contractors used in security administration are prohibited from performing certain critical, closely associated roles with inherently governmental, or otherwise exempt functions and activities that cannot or should not be performed by a contractor in accordance with volume 1, "Use of Contractors in Security Administration" of reference (f).

e. Prohibit the use of foreign nationals in security administration in accordance with volume 1, "Use of Foreign Nationals in Security Administration" of reference (f).

f. Ensure all assigned personnel have a valid and appropriate security clearance, have executed an appropriate non-disclosure agreement, and have a valid need-to-know before allowing access to classified information. Refer to volume 1, "Access to Classified Information" of reference (f) for more information.

g. Ensure all persons with access to classified information systems (e.g., SIPRNet, collateral TS networks, etc.) receive the NATO briefing and responsibilities for safeguarding NATO classified information, and acknowledge receipt of the brief in writing:

(1) Mass briefing sign-in rosters are not sufficient and may not serve as written acknowledgement of the brief.

(2) For JWICS access requirements, consult the activity's SSO and follow DNI policy requirements.

h. Ensure classified information and CUI are protected in accordance with this instruction, volumes 1 through 4 of reference (f), and any of its implementing policies.

i. Ensure prompt and appropriate management action is taken in cases of compromise, UD, or loss of classified information or CUI. Report any violation of this instruction, or one of its implementing directives, that results in negligence or willful disclosures of classified information or CUI, as determined by a PI, management inquiry (for CUI), or investigation in JPAS, or its successor system. Refer to volume 1, "Corrective Actions

and Sanctions" and section 1k of enclosure (3) of volume 4 of reference (f), and paragraph 10 of reference (t) for more information.

j. Ensure their personnel, prior to accessing a classified information system, receive derivative classification training as specified in volume 1, "Derivative Classification, Responsibilities of Derivative Classifiers, and Procedures for Derivative Classification" and volume 3, "Initial Orientation" of reference (f) and annually thereafter. For additional information on this training contact a supervisor, manager, commander, or activity security manager.

k. Not take retribution against any individual for questioning a classification or making an informal or formal challenge to a classification.

l. Ensure personnel under their authority mark derivatively classified documents with banner lines, portion markings, and classification authority block in accordance with volume 2, "Marking Principles" of reference (f). Figures 1 through 58 of reference (f) are examples of marking most types of derivate classified documents and material. Figure 4 of reference (f) is an example of a derivatively classified document.

m. Ensure personnel properly mark classified files, folders, and similar groups of documents, and IT systems in accordance with volume 2, "Coversheets and Classification Labels" of reference (f).

n. Ensure personnel properly create, mark, protect, and destroy working papers in accordance with volume 3, "Working Papers" of reference (f). Figure 11 of volume 2, "Marking Principles" of reference (f), is an example of marking a working paper.

o. Ensure personnel under their authority completely destroy classified documents and material identified for destruction to prevent anyone from reconstructing the classified information using only the method and equipment identified in volume 3, "Destruction of Classified Information and Destruction Procedures" of reference (f).

p. Ensure personnel are familiar with and follow the transmission and transportation procedures in "Transmission and Transportation" of volume 3 of reference (f). Use of the current holder of the GSA contract for overnight delivery is authorized.

q. Train their personnel on reporting and notification procedures in the event anyone finds classified information out of proper control in accordance with the procedures identified in "Reporting and Notifications" of volume 3 of reference (f).

r. Train their personnel on proper notification procedures when they discover classified information in the public media in accordance with volume 3, "Information Appearing in the Public Media" of reference (f).

s. Train personnel assigned to a program employing ACCM on the procedures for safeguarding and marking ACCM material in accordance with the OCA's guidelines and volume 3, "Alternative Compensatory Control Measures (ACCM)" and volume 2, "Other Dissemination Control Marking: Alternative Compensatory Control Measures (ACCM)" of reference (f).

t. Enforce prohibition of personally owned electronic devices (unmanaged government devices) in open storage rooms (secure rooms), SCIF, SAPF, classified meetings, conferences, or other forums where classified information is to be discussed or processed. Finally, heads of activities should consider whether to restrict personally owned electronic devices in meetings, conferences, or other forums where CUI is to be discussed or processed.

20. All DON Personnel (i.e., military, civilian, and contractor) shall:

a. Be personally and individually responsible for properly protecting classified information and CUI under their custody and control.

b. Have a valid and appropriate security clearance, have executed an appropriate non-disclosure agreement, and have a valid need-to-know before allowing access to classified information. Refer to volume 1, "Access to Classified Information" of reference (f) for more information.

c. When authorized access to classified information systems (e.g., SIPRNet, collateral TS networks, etc.), acknowledge in writing that they have received the NATO briefing and responsibilities for safeguarding NATO classified information.

(1) Mass briefing sign-in rosters are not sufficient and may not serve as written acknowledgement of the brief.

(2) For JWICS access requirements, consult the activity's SSO and follow DNI policy requirements.

d. Ensure classified information and CUI are protected in accordance with this instruction, volumes 1 through 4 of reference (f), and any of its implementing policies.

e. Report all security incidents to their supervisor, management, commander, or activity security manager.

f. May submit tentative classified information to an OCA for original classification decisions by submitting the required information in volume 1, "Original Classification Process" of reference (f). Contact the activity security manager for additional assistance. Safeguard the information at the specified level of classification and do not use as a source document for derivative classification.

g. Prior to accessing a classified information system receive derivative classification training as specified in volume 1, "Derivative Classification, Responsibilities of Derivative Classifiers, and Procedures for Derivative Classification" and volume 3, "Initial Orientation" of reference (f) and annually thereafter. For additional information on this training contact a supervisor, manager, head of the activity, or activity security manager.

h. Make informal and formal classification challenges when they believe information is improperly or unnecessarily classified and communicate that belief to their supervisor and activity security manager; protect the information at its current classification level or the recommended change level, whichever is higher until a decision is made and process informal and formal challenges in accordance with volume 1, "Challenges to Classification" of reference (f) through the chain of command to the OCA.

i. Mark derivatively classified documents with banner lines, portion markings, and classification authority block in accordance with volume 2, “Marking Principles” of reference (f). Figures 1 through 58 of reference (f) are examples of marking most types of derivatively classified documents and material. Figure 4 of reference (f) is an example of a derivatively classified document.

j. Properly mark classified files, folders, and similar groups of documents, and IT systems in accordance with volume 2, “Coversheets and Classification Labels” of reference (f).

k. Be personally responsible for taking proper precautions to ensure that unauthorized persons do not gain access to classified information and for protecting the classified information they know, possess, or control, and comply with the pre-publication security review processes prior to publishing any document. Refer to volume 3, “Personal Responsibility for Safeguard” of reference (f) for additional information.

l. Keep classified material removed from storage under constant surveillance and covered with coversheets when not in secure storage. Refer to volume 3, “Protection When Removed from Storage” of reference (f) for additional details on coversheets.

m. Properly create, mark, protect, and destroy working papers in accordance with volume 3, “Working Papers” of reference (f).

n. Destroy classified documents and material identified for destruction completely, to prevent anyone from reconstructing the classified information using only the methods and equipment identified in volume 3, “Destruction of Classified Information and Destruction Procedures” of reference (f).

o. Transmit or transport classified information using the procedures in volume 3, “Transmission and Transportation” of reference (f). Use of the current holder of the GSA contract for overnight delivery is authorized.

p. Take custody of and safeguard classified information when found out of proper control and report the matter to their supervisor and/or activity security manager using appropriate

communications methods or face-to-face whenever possible. If the head of the activity or the activity security manager are involved in or responsible for the incident, report the incident to activity security manager or head of the activity at the next higher level of command or supervision.

q. Not make any statement or comment that confirms or denies the accuracy of or verifies information requiring protection that appears in the public media, including on public internet sites, or if approached by a representative of the media. Report the matter immediately to your supervisor and activity security manager.

r. Notify their supervisor and/or activity security manager whenever they observe classified information in the public media as quickly as possible. The information to report can be found in volume 3, "Information Appearing in the Public Media" of reference (f). Report as much information as possible.

s. Ensure computer media is properly disposed of in accordance with volume 3, "Disposal of Computer Media" of reference (f).

t. Ensure ACCM information is properly safeguarded in accordance with the OCA instructions and volume 3, "Alternative Compensatory Control Measures (ACCM)" and ACCM documents and material are marked in accordance with volume 2, "Other Dissemination Control Marking: Alternative Compensatory Control Measures (ACCM)" of reference (f).

u. Not take personally owned electronic devices into open storage rooms (secure rooms), SCIFs, or SAPFs, or use them during classified meetings, conferences, or other forums where classified information is to be discussed or processed.

21. All DON OCAs shall:

a. Not delegate OCA to any other person or position. Refer to volume 1, "Requests for OCA" of reference (f).

b. Before exercising their authority and annually thereafter, certify in writing that they have received training in:

(1) The fundamentals of proper security classification and declassification.

(2) The limitations of their authority.

(3) The sanctions that may be imposed.

(4) OCA duties and responsibilities as required by volume 3, “OCA Training” of reference (f).

c. Provide written certification of training to the activity security manager, who shall provide the training certifications when requested by appropriate authorities (e.g., SAO, USD (I), ISOO, etc.).

d. Only classify information to protect national security in accordance with volume 1, “Classification Policy and Classification Prohibitions” of reference (f).

e. Only classify information using the levels of classification identified in volume 1, “Level of Classification” of reference (f).

f. Make original classification decisions commensurate with the process identified in volume 1, “Original Classification and Original Classification Process,” of reference (f).

g. Only make changes to the level of classification of information under their jurisdiction following the procedures in volume 1, “Changing the Level of Classification,” of reference (f).

h. Issue and disseminate security classification guidance for each system, plan, program, project, or mission involving classified information under their jurisdiction:

(1) The primary DON vehicle for issuing classification guidance is the SCG. Refer to volume 1, “Security Classification Guidance, Challenges to Classification, and Security Classification Guides,” of reference (f) for content details.

(2) Classification guidance may be issued in the form of a memorandum, plan, order, or letter when it is determined that

development of an SCG is not appropriate (e.g., exercises, military operations less than one year, etc.).

(3) SECNAV, USN, and USMC publications may not be used to issue security classification guidance. Remove all security classification guidance from any SECNAV, USN, or USMC publication within 180 days from the date of this instruction.

i. Make final classification decisions within 180 days from the initial drafting date of any document or material received under the tentative classification process. Refer to volume 1, “Tentative Classification” of reference (f) for additional details.

j. Establish the shortest duration of classification of information by identifying a specific date or event for declassification based on the guidelines in volume 1, “Duration of Classification” of reference (f).

k. Identify elements of unclassified information that when compiled (aggregated) reveals an additional association or relationship that qualifies for classification at the TS, secret, or confidential level. Note that user queries of data in electronic formats (e.g., databases, spreadsheets) lead to new aggregations, and posting of information on the Internet makes the use of data mining and other data correlation tools easy and widespread. Refer to volume 1, “Compilations” of reference (f) for additional details.

l. Immediately review any information released to the public without proper authority (i.e., media leak, data spill, classified message incident, etc.) or when notified of a compromise as a result of security incident to determine if declassification is appropriate or to address additional protection requirements. In addition, only reclassify information released to the public under proper authority when necessary. Refer to volume 1, “Classification of Information Released to the Public” and volume 3, “Actions to be Taken by the OCA” of reference (f) for resolving compromises of classified information involved in security incidents.

m. Complete damage assessments within DoD goal of six months from the first date the compromise was declared.

n. Submit requests for classification or reclassification following receipt of a request for information through the SAO to USD (I). Refer to volume 1, “Classification or Reclassification Following Receipt of a Request for Information” of reference (f).

o. Not classify information that is a product of contractor or individual independent research and development or bid and proposal efforts conducted without prior or current access to classified information associated with the specific information unless the requirements of volume 1, “Classifying Non-Government Research and Development Information” of reference (f) are met.

p. Process patent applications that contain information that warrants classification in accordance with volume 1, “The Patent Secrecy Act of 1952” of reference (f).

q. Not take retribution against any individual for questioning a classification or making a formal challenge to a classification.

r. Respond to formal classification challenges within prescribed timelines identified in volume 1, “Challenges to Classification” of reference (f). In addition, allow for sufficient time for the SAO to conduct an impartial review.

s. Request exemptions from automatic declassification in accordance with volume 1, “Exemptions from Automatic Declassification” of reference (f) through the DON/AA Declassification Office.

t. Have authority to declassify or downgrade information that they have originally classified and have jurisdiction over. Refer to volume 1, “Authority to Declassify,” of reference (f). Complete declassification and downgrade of information in accordance with volume 1 of reference (f). In addition:

(1) Supervisors of an OCA, may declassify or downgrade information originally classified by a subordinate OCA provided they have jurisdiction over the information and have OCA. Otherwise, refer the decision to the SAO through command channels.

(2) OCAs may designate members of their staffs to exercise declassification authority over information under their jurisdiction provided these members have received training as specified in volume 3, “Declassification Authority Training” of reference (f).

(3) OCAs are not authorized to declassify FGI without the prior consent of the originating government. Refer to volume 1, “Declassifying FGI” of reference (f).

u. Work closely with the DON Declassification Authority to develop the department’s declassification guide. Refer to volume 1, “Automatic Declassification, Exemptions from Automatic Declassification, Declassification of Information Marked with Old Declassification Instructions, and Systematic Declassification” of reference (f).

v. Downgrade classified information to a lower level of classification when the information no longer requires protection at the originally assigned level and can be properly protected at a lower level. Refer to volume 1, “Downgrading Classified Information” of reference (f). Do not downgrade FGI without the prior consent of the originating government. Refer to volume 1, “Declassifying FGI” of reference (f).

w. Upgrade classified information to a higher level of classification, provided the OCA have delegated authority to do so, it benefits national security, and the OCA has the ability to notify all holders of the information of the change so that the information can be safeguarded at the higher level. Refer to volume 1, “Upgrading Classified Information” of reference (f).

x. Mark originally classified documents in accordance with Figure 3, “Marking Principles” of volume 2 of reference (f). Figures 1 through 58 of reference (f) are examples of marking most types of classified documents and material created in the DON.

y. Submit requests to use ACCM through command channels to the SAO for approval. Address the elements in volume 3, “Alternative Compensatory Control Measures (ACCM): ACCM Approval, Guidance on ACCM Use, and Documentation” of reference (f). In addition:

(1) Ensure ACCMs do not employ any of the prohibited security measures identified in volume 3, “Alternative Compensatory Control Measures (ACCM): Prohibited Security Measures or Prohibited Uses of ACCM” of reference (f).

(2) Develop and distribute a program security plan, SCG, and program participant briefing to all participating organizations prior to the activation of the ACCM in accordance with volume 3, “Alternative Compensatory Control Measures (ACCM): Documentation” of reference (f).

(3) Respond to annual report requests from the SAO.

(4) Only share ACCM-protected information with DON organizations, DoD Components, and/or Federal government departments and agencies only when the recipient organization agrees to abide by the ACCM security requirements stipulated in Enclosure (2) of volume 3 of reference (f).

(5) Only authorized DoD contractors may participate in ACCM provided access and the associated security plan are identified in the DD Form 254, “Contract Security Classification Specification.”

(6) Ensure primary and alternate ACCM control officers for each organization managing an ACCM are identified.

(7) Ensure ACCM are safeguarded and administered in accordance with volume 3, “Alternative Compensatory Control Measures (ACCM): Safeguarding ACCM Information” of reference (f).

(8) Ensure ACCM material is marked in accordance with volume 2, “Other Dissemination Control Marking: Alternative Compensatory Control Measures (ACCM)” of reference (f).

(9) Terminate ACCM when these security measures are no longer required through the chain-of-command to the SAO. The termination must be writing.

22. Derivative Classifier. All DON derivative classifiers must:

a. Be trained initially, and annually thereafter, on proper procedures for making classification determinations and properly marking derivatively classified documents.

b. Be familiar with their responsibilities and procedures for derivative classification. Refer to sections 10 and 11 of enclosure (4) of volume 1 of reference (f).

c. Mark derivatively classified documents in accordance with volume 2 of reference (f).

23. ACCM Control Officer. Serves as the organization's point of contact for all matters concerning ACCM. ACCM Control Officers:

a. Maintain an updated ACCM access control list for their organization.

b. May authorize action officer to action officer contact once access control lists have been exchanged between organizations.

c. Ensure ACCM are safeguarded in accordance with volume 3, "Alternative Compensatory Control Measures (ACCM): Safeguarding ACCM Information," of reference (f).

d. Ensure ACCM material is marked in accordance with volume 2, "Other Dissemination Control Marking: Alternative Compensatory Control Measures (ACCM)," of reference (f).

24. Escorts and Couriers. DON military and U.S. government civilian escorts and couriers shall:

a. Only escort or courier classified information when in possession of an authorization statement. Contact the activity security manager for guidance on obtaining an authorization statement.

b. Be briefed by the head of activity or activity security manager on their security responsibilities prior to hand-carrying, couriering, or escorting classified information. Refer to volume 3, "Responsibilities" of reference (f) for addition requirements.

c. Ensure the classified material is properly packaged in accordance with volume 3, “Preparation of Material for Shipment and Packaging Requirements” of reference (f) prior to escorting or couriering the information.

d. Hand-carry classified information aboard a U.S. carrier, or a foreign carrier if no U.S. carrier is available, provided the escort or courier retains custody and physical control of the information at all times.

e. Make arrangements for secure storage of the information at a U.S. Government or cleared U.S. contractor facility.

f. Coordinate with Transportation Security Administration field office in unusual situations to facilitate clearance through airline screening processes in accordance with volume 3, “Hand-Carrying or Escorting Classified Information on Commercial Aircraft” of reference (f).

g. Make arrangement with customs, police, and immigration officials in advance to facilitate movement through security and take actions consistent with measures in volume 3, “Customs, Police, and Immigration” of reference (f) when such officials inquire into the contents of the package or other container the classified information is being transported in.

h. Only transfer classified information and material to a foreign government or international organization when an agreement is in-place only through official government-to-government channels as outlined in Appendix to enclosure (4) of volume 3, “Transfer of Classified Information or Material to Foreign Governments” of reference (f). Receipts are required for all transfers of classified information and material to a foreign government, unless exempted per the reference in this paragraph.

25. PI Officials. All persons designated as PI officials for addressing security incidents involving classified information by the head of the activity or activity security manager will:

a. Classify PI reports in accordance with volume 3, “Classification of Reports” of reference (f).

b. Ensure certain types of classified information or specific circumstances are addressed using unique handling or consideration of additional reporting requirements as defined in volume 3, “Special Circumstances,” of reference (f).

c. Notify the appointing authority (normally, the head of the activity) or activity security manager when a PI reveals information suggestive of a criminal or CI nature is discovered and cease all actions pending coordination with appropriate authorities as outlined in volume 3, “Security Inquiries and Investigations,” of reference (f).

d. Immediately notify the appointing authority or activity security manager if the PI official determines a loss or compromise has occurred.

e. Complete the PI as soon as possible, not to exceed 10 duty days. If the PI cannot be completed within 10 duty days request an extension from the appointing authority.

f. Obtain information to provide answers to the questions identified in volume 3, “Security Inquiries and Investigations,” of reference (f). Such information shall be sufficient to resolve the incident.

g. Complete a report of findings and provide it to the appointing authority (head of the activity or security manager). Do not recommend punitive action against the individual(s) responsible for the infraction or violation. This is the responsibility of the appropriate military commander or management official. Document the results of the command investigation using the format in volume 3, “Security Incident Reporting Format” of reference (f) or another format proscribed by the head of the activity head or the activity security manager.

26. Investigating Officials. All investigating officials will be designated in writing by the head of the activity for the purpose of investigating a security incident related to classified information. Investigating officials:

a. Classify reports in accordance with volume 3, “Classification of Reports” of reference (f).

b. Ensure certain types of classified information or specific circumstances are addressed using unique handling or consideration of additional reporting requirements as defined in volume 3, “Special Circumstances” of reference (f).

c. Notify the appointing authority (normally, the head of the activity) or activity security manager when a command investigation reveals information suggestive of a criminal or CI nature is discovered and cease all actions pending coordination with appropriate authorities as outlined in volume 3, “Security Inquiries and Investigations” of reference (f).

d. Immediately notify the appointing authority or activity security manager if the investigating official determines a loss or compromise has occurred.

e. Obtain information to provide answers to the questions identified in volume 3, “Security Inquiries and Investigations” of reference (f). Such information shall be sufficient to resolve the incident.

f. Provide recommendations for any corrective or disciplinary actions.

g. As needed, consult with local legal counsel to ensure any evidence developed that could be used in an administrative or disciplinary actions would be admissible.

h. Document the results of the command investigation using the format in volume 3, “Security Incident Reporting Format” of reference (f) or another format proscribed by the head of the activity or the activity security manager.

DEPARTMENT OF THE NAVY INFORMATION SECURITY PROGRAM OVERVIEW

1. Purpose. The purpose of the DON ISP is to ensure classified and controlled CUI is properly created, safeguarded, transmitted, and destroyed. This is referred to as the lifecycle for classified information and CUI. Refer to volume 4 of reference (f) for creating, safeguarding, and destruction of CUI.

a. Information will not be classified, continue to be maintained as classified, or fail to be declassified, or be designated CUI under any circumstances in order to:

(1) Conceal violations of law, inefficiency, or administrative error.

(2) Prevent embarrassment to a person, organization, or agency.

(3) Restrain competition.

(4) Prevent or delay the release of information that does not require protection in the interests of national security or as required by statute or regulation.

b. Declassification of classified information will receive equal attention as the classification of information so that information remains classified only as long as required by national security considerations.

c. The volume of CNSI and CUI retained, in whatever format or media, must be reduced to the minimum necessary to meet operational requirements.

2. Templates to this Enclosure. All templates referenced in this enclosure can be found on the Information Security SharePoint web portal.

3. Creating Classified Information. There are three processes for creating classified information: original, tentative, and derivative. Refer to enclosure (4) of this instruction for specific information on these processes.

4. Safeguarding Classified Information. All DON personnel (i.e., military, civilian, and contractor) who work with classified information are personally responsible for taking proper precautions to ensure that unauthorized persons do not gain access to classified information and the information they know, possess, or control is properly safeguarded in accordance with this instruction and its implementing directives.

a. Heads of DON Activities

(1) May submit waivers and exceptions through the chain-of-command, using the "Waiver or Exception to Standard or Requirement Template" or "Waiver to Marking Standard or Requirement Template" to the DON SAO when situations arise that require deviation from the standards of this instruction or any of its implementing directives.

(2) When special circumstances exist, may authorize the use of key operated locks for storing bulky material containing secret and confidential information provided:

(a) The authorization is documented with an explanation of the special circumstances and administrative procedures are established for control and accounting of keys and locks.

(b) The keys shall be protected at the level of the classified bulky material.

(3) Must ensure management takes prompt and appropriate action with a focus on correcting or eliminating the conditions that caused or brought about a security incident in cases of:

(a) Compromise of classified information and UD of CUI.

(b) Improper classification or designation of information.

(c) Violation of the provisions of this instruction or any of its implementing directives.

(d) Incidents that may put classified information and CUI at risk or UD.

(4) May approve classified meetings and conferences in U.S. cleared government facilities they have control over or if held in a cleared U.S. contractor facility that has an appropriate facility security clearance and, as required, secure storage capability provided:

(a) The meeting or conference serves a specified U.S. government purpose.

(b) Other approved methods or channels for disseminating classified information or material are insufficient or impractical.

(c) An official is assigned as a security manager to address security provisions identified in sections 16b and 16c of Enclosure (2) of volume 3 of reference (f).

(d) Signed agreements between foreign governments that the responsible foreign government will agree to use security measures and controls that are at least as stringent as those required by this instruction and any of its implementing directives and are in place prior to the event. Section 16d to above stated reference in paragraph 4a(4)(c) shall be satisfied as well.

(5) Will submit exception to policy to paragraph 4a(4) above, using the “Classified Off-Base Conference Request Template,” when facilities other than appropriately cleared U.S. government or U.S. contractor facilities are proposed for use to the SAO for approval. If approved, the head of the DON activity must submit an after-action report within 90 days to the DUSN via the DUSN Security Directorate. Prior to submitting an exception, conduct a risk assessment and assess the threat to classified information. The submission must:

(a) Be received a minimum of 15 business days prior to the event.

(b) Identify an official who shall serve as the security manager for the event.

(c) Identify the level of classification to be discussed.

(d) Contain a risk acceptance statement.

(e) Include a security plan that describes how the requirements of volume 3, “Classified Meetings and Conferences” of reference (f) shall be met.

(f) Signed agreements between foreign governments that the responsible foreign government will agree to use security measures and controls that are at least as stringent as those required by this instruction and any of its implementing directives.

(6) Ensure organization personnel secure classified information adequate to deter and detect access by unauthorized persons by following the guidance in volume 3, “Storage and Destruction” of reference (f).

(7) Ensure a risk assessment is performed and addresses the minimum standards identified in volume 3, “Risk Assessment” of reference (f) to aid in identification and selection of supplemental controls that may need to be implemented.

(8) Restrict the transporting (hand-carried) of classified information to the greatest extent possible and only authorize it when it is not practical to transmit classified information by approved classified information system(s).

(9) Ensure all assigned personnel receive security education and training that provides necessary knowledge and information to:

(a) Enable quality performance of security functions.

(b) Promote understanding of the DON and the DoD ISP policies and requirements and their importance to national security and national interests.

(c) Instill and maintain continuing awareness of security requirements.

(d) Assist in promoting a high degree of motivation to support program goals.

(10) Ensure when specified security functions are performed by or for other activities, enter into a Security Servicing Agreement (SSA), be that a memorandum of understanding or memorandum of agreement, signed by the head of each activity affected. The "Servicing Security Agreement Template" is provided to assist the activity in developing its SSA.

b. DON Activity Security Managers. Serves as the principal advisor and representative to the head of the activity, management, and personnel on all matters related to the DON ISP. DON activity security managers shall:

(1) Provide guidance to all personnel on administering the DON ISP and if needed, elevate issues through the chain-of-command to DUSN Security.

(2) Develop emergency plans, instructions, procedures to address areas identified in volume 3, "Emergency Plans, Equipment Used for Processing Classified Information, and Reproduction of Classified Material" of reference (f). The "Emergency Plan Template" is provided to help security managers in their all-threats emergency planning efforts.

(3) Ensure activity personnel are securing classified information adequately to deter and detect access by unauthorized persons by following the guidance in volume 3 of reference (f), or the activities local policy.

(4) Conduct, or assist others in conducting, risk assessment to meet the minimum standards identified in volume 3, "Risk Assessment" of reference (f) to aid identification and selection of supplemental controls that may need to be implemented. The "Risk Assessment Template" is provided as an example to assist in the risk assessment process.

(5) Train personnel on their responsibilities for transporting (hand-carry) classified information and ensure they possess the proper credentials as required.

(6) Will ensure heads of activities and activity personnel are advised on purchasing and use of equipment for destruction of classified and CUI. Refer to volume 3, "Technical Guidance on Destruction Methods" of reference (f) for additional information.

(7) Ensure activity personnel assigned to conduct preliminary inquiries use the “Preliminary Inquiry Report Template” to record those required elements of sections 6d(4)(a) through (i).

(8) Ensure command personnel assigned to conduct command investigations use the “Command Investigation Report Template” to record those required elements of section 0208 of enclosure (1) of reference (ac) and section 6e(4) of enclosure (6) of volume 3 of reference (f).

c. All DON Personnel (i.e., military, civilian, and contractors) must:

(1) Clearly mark, designate, or electronically label all classified and CUI in accordance with volumes 2 and 4 of reference (f) to alert holders of the classification level and protection standards of the information. When in doubt on how to mark classified documents, contact the activity security manager.

(2) Ensure organization personnel are aware of policies and procedures to secure classified information and designated secure spaces, and prevent loss or compromise, to deter and detect access by unauthorized persons by following the guidance in volume 3 of reference (f).

(3) Grant access to only those individuals that have an appropriate security clearance, a signed SF 312 or similar document if granted access to SCI or a SAP, and a need-to-know. Contact the DON activity security manager when in doubt or assistance is needed.

(4) Not take classified home for work unless authorized by the appropriate official and safeguards are in place to protect the information.

(5) Only process classified material on approved classified information systems.

(6) Validate visitors to a DON facility have their identity, security clearance and access, and need-to-know verified prior to the visit. Unannounced visitors will not be allowed entry to a facility where access to, or where disclosure

of, classified information may occur until their identity, security clearance and access level and need-to-know are verified. Do not deny access until the activity security manager or head of the activity has been advised.

(7) Report security incidents to their activity security manager or the head of the activity.

(8) Contacting the activity security manager or head of the activity when in doubt on implementing any portion of this instruction or its implementing directives.

5. Destruction of Classified and CUI

a. Classified information and CUI documents and material identified for destruction must be destroyed completely, to prevent anyone from reconstructing the information, according to procedures and methods in volumes 3 and 4 of reference (f).

b. Within the DON, all classified information and CUI intended for destruction will only be destroyed by authorized means and appropriately cleared personnel.

c. Establish at least one day each year when specific attention and effort is focused on disposing of unneeded classified material (clean-out day).

d. All DON personnel will destroy classified information and CUI in a manner to minimize the possibility of unauthorized removal and/or access. Only approved equipment or methods may be used for destruction, which must first be verified by the head of the activity or the activity security manager.

e. Use of the “Classified Material Destruction Device Certificate Template” is recommended, to ensure the requirements of sections 17d and 17d(2) and (3) of enclosure (3) of volume 3 of reference (f) are met.

f. Ensure the OPNAV 5511-12 (Rev. 8-75), “Classified Material Destruction Report,” is used to satisfy the requirements of section 10a of enclosure (2) of volume 1 of reference (f) is met.

CLASSIFICATION MANAGEMENT

1. General

a. Original classification

(1) Is an initial decision that an item of information could reasonably be expected to cause identifiable or describable damage to the national security if subjected to UD and requires protection in the interest of national security is called original classification. The SCG is the DON tool for OCA to convey original classification decisions; furthermore, the "SCG Format and Preparation Template" is the DON authorized SCG format.

(2) SCGs serve both legal and management functions by recording OCA determinations made under references (f) and (ag). They are also the primary reference for derivative classifiers to identify the level and duration of classification for specific information elements, to include alternative compensatory control measures; identify unclassified information meeting the protection requirements of volume 4 of reference (f) and may include special public release requirements and foreign disclosure considerations.

b. Tentative Classification. Tentative Classification is the process of classifying information, such as working papers, and submitting the information or document to an OCA for approval. This information shall be safeguarded as any other classified information until an OCA's decision is made, but not later than 180 days from the initial drafting date of the document. Refer to volume 1 of reference (f) for additional information.

c. Derivative Classification. Is the process of taking existing classified information, based on classification guidance in a SCG or other source material, and incorporating, paraphrasing, restating, or generating classified information in a new form or document. Photocopying, or mechanically or electronically reproducing classified material is not derivative classification. Persons that use this methodology are called derivative classifiers.

d. DON SCG Program. This program is a services-managed repository for service-specific DON SCGs.

(1) DON SCGs are issued by their representative OCA and indexed under one of the following major standardized subject identification codes (SSIC):

(a) 5513.2: Air Warfare Systems;

(b) 5513.3: Surface Warfare Systems;

(c) 5513.4: General Intelligence, Cover and Deception, Security and Investigative Programs;

(d) 5513.5: Undersea Warfare Program;

(e) 5513.6: Communications and Satellite Program;

(f) 5513.7: Mine Warfare Program;

(g) 5513.8: Electronic Warfare Program;

(h) 5513.9: N uclear Warfare Program;

(i) 5513.10: Advanced Technology and Miscellaneous Programs;

(j) 5513.11: Marine Corps Ground Combat and Miscellaneous Programs;

(k) 5513.12: Intelligence Research Projects;

(l) 5513.13: Non-Acoustic Anti-Submarine Warfare Program; or

(m) 5513.15: Naval Special Warfare Program.

(2) The index of DON SCGs, by SSIC, were previously issued as a series of instructions, the OPNAV Instruction (OPNAVINST) 5513 series. During 2016, the OPNAVINST 5513 series was cancelled. Although the OPNAVINST 5513 series has been cancelled, the index by SSIC and sequential identification number assigned are retained. Newly created or revised SCGs may not reference the OPNAVINST 5513 series.

e. Declassification. In accordance with the provisions of section 3.7 of reference (b), the DON will comply with guidelines set by the National Declassification Center within the National Archives for streamlining declassification processes, facilitating quality assurance measures, and implementing standardized training regarding the declassification of records determined to have permanent historical value.

f. Classification Challenges. If holders of information have substantial reason to believe that the information is improperly or unnecessarily classified, they shall communicate that belief to their security manager or the OCA to bring about any necessary correction. This may be done informally or by submitting a formal challenge to the classification. Informal questioning of classification is encouraged before resorting to formal challenge.

g. All templates referenced in this enclosure can be found on the Information Security SharePoint web portal.

2. Designation of OCAs. Comply with enclosures (4) and (6) of volume 1 of reference (f), enclosures (2) and (3) of reference (ah), and the requirements outlined in this enclosure.

a. OCA within the DON is delegated by position.

b. A TS OCA may make lower classification decisions at the secret and confidential levels. A secret OCA may only make secret and confidential classification decisions.

c. Only persons who have a demonstrable and continuing need to exercise OCA during the normal course of operations may be delegated OCA:

(1) To meet the test for demonstrable and continuing need, an OCA must maintain a SCG, or absent a SCG, an OCA must exercise their authority an average of twice a year.

(2) All requests for secret OCA will be submitted to the DUSN via the DUSN Security Directorate using the “Request for Delegation of Secret OCA Template.” All requests for TS OCA will be submitted to the SECNAV via the DUSN Security

Directorate using the “Request for Delegation of TS OCA Template.”

3. Preparation of the SCG

a. General. DON SCGs will conform to the classification management principles described in enclosures (2) and (3) of reference (ah). The “SCG Format and Preparation Template” is the official DON format for SCGs and describes the minimum data required to be included. A copy of the template can be found on the DUSN Information Security web site:

(1) The SCG format should be tailored to fit a particular program’s need (i.e., if a section in the template does not apply to the program, omit it from the SCG).

(2) The appropriate special notice(s), as defined in section 4 of enclosure (3) of volume 2 of reference (f), will be applied to the face of each SCG; at a minimum, each SCG shall have affixed to the face and at the bottom left of the document a distribution statement, as SCGs are considered technical documents.

(3) Classified SCGs shall have a classification authority block applied to the face of the document directly under the last special notice. The classification authority block shall contain those elements described at sections 8b(1) through (5) of enclosure (3) of volume 2 of reference (f).

(4) As SCGs serve to convey original classification decisions vice readdress established policy, SCGs shall not include the categories specified in subsections 1.4(a) through 1.4(h) of reference (b) or sections 2a(3)(a) thru 2a(3)(h) of enclosure (2) of reference (ah) nor shall there be included any instructions already spelled out in volumes 2 through 4 of reference (f) (i.e., general marking requirements or shipping instructions, etc.).

b. Developing a New SCG

(1) The OCA staff, along with the security staff supporting the OCA shall work together to develop SCGs. The OCA will ensure the policy requirements of reference (ag) and

enclosure (6) of volume 1 of reference (f), and this enclosure are followed.

(2) The classification block of the SCG will only be populated with "(U)," "(C)," "(S)," or "(TS)" as these are the only classification markings authorized:

(a) If the OCA determines an item requires protection under the controlled CUI program then mark the "CLASSIFICATION" block, "(U) SEE REMARKS." In the "REMARKS" column place "FOUO" or "CUI" when new guidance is published for the full implementation of the CUI Program.

(b) If the OCA determines an item requires classification at multiple levels, place the levels in the "CLASSIFICATION" block and annotate "SEE REMARKS." Example: "(U)-(S) SEE REMARKS." In the "REMARKS" block specify when each classification is "(U)," "(C)," and "(S)."

(3) For all classified line items, the "REASON" block must be annotated with the appropriate classification category(ies) in section 1.4 of reference (b). The "REASON" block will not be annotated for unclassified line items.

(4) The "DECLASSIFICATION" block will be annotated with either:

(a) A date within 10 years. If a date within 10 years cannot be established, determine if the line item can be declassified at the 10 year mark. If declassification beyond 10 years is required move to the next step below.

(b) A date within 25 years. If a date within 25 years cannot be established, then the line item must be declassified at 25 years. Exception: A line item may be extended past 25 years provided an exemption has been approved by Interagency Security Classification Appeals Panel (ISCAP). DON/AA Declassification Office processes exemptions for all DON OCAs and SCGs. Refer to section 13b of enclosure (5) of volume 1 of reference (f) for a list of exemptions.

(c) An event. Example: when vulnerability is mitigated.

c. Compilation. Compilations (aggregations) of information that are individually unclassified (or classified at a lower level) may be classified (or classified at a higher level) only if the compiled information reveals an additional association or relationship that qualifies for classification and is not otherwise revealed by the individual elements of information:

(1) Determine if any unclassified or CUI within a SCG, when compiled, will raise the unclassified or CUI to classified levels. For example, line item "a" is CUI. Line item "b" is CUI. When line item "a" and "b" are compiled in a document, record, website, etc., the classification level becomes SECRET.

(2) Determine if any classified information at the secret or confidential levels when compiled with other classified, unclassified, or CUI would increase the level of protection. For example: line item "a" is SECRET. Line item "b" is CUI. When compiling line item "a" and "b" in a document, record, website, or etc., the classification level becomes TS.

4. Review. The SCG should be reviewed by all senior level activity security staff. Once the final senior level security staff has completed their review and all corrections are made, notify the Service DON SCG Program Manager and request an SCG Identification Number, and complete the Directives Division (DD) Form 2024, "DoD SCG Data Elements," in preparation for the OCA signature.

5. OCA Signature. Once the SCG Identification Number has been received, the OCA signs the SCG and DD Form 2024. Once the SCG is signed, the senior security official will disseminate the SCG and DD Form 2024.

a. One copy of the signed SCG and its associated DD Form 2024 must be sent to the Service DON SCG Program Manager, DUSN Security Directorate, and the DON/AA Declassification Office. Whenever possible, disseminate the SCG and DD Form 2024 by Non-secure Internet Protocol Router Network, SIPRNet, or JWICS.

b. One copy of the signed SCG and its DD Form 2024 are distributed in accordance with the rules of section 6 of enclosure (6) of volume 1 of reference (f). The Service security office will develop policy to ensure the DTIC distribution prohibitions of section 6c are not violated.

c. Each Service shall develop retention and distribution protocols for classified SCGs containing information elements protected under alternative compensatory control measures.

6. Revising an SCG. Follow the same procedures for developing an SCG when revising an SCG. An SCG should only be revised to annotate "new" classification decisions of "new line items," extend declassification decisions less than 25-years to a maximum of 25-years, or to annotate receipt of an approved ISCAP exemption to declassification.

a. Never revise the declassification dates of existing line items when those line items are annotated at the 25-year mark. For example: An SCG dated 20181017 with a declassification date of 20431017 cannot be revised beyond the 25-year mark without an approved ISCAP exemption. However, if the declassification date is less than 25 years, the OCA may revise the classification date out to 25 years.

b. New line items may be declassified up to 25 years from the revision date. The only exception to this rule is if the OCA receives an approved ISCAP exemption.

7. Fundamental Classification Guidance Reviews. SCGs shall be reviewed every five years, or sooner, by the OCA. The clock for the review starts the date the OCA approved the SCG.

a. If no revisions to the SCG are made, the OCA annotates the date of review on the cover of the SCG and signs or initials. The clock for the next review restarts.

b. If there are revisions, process them in the same manner for developing/revising an SCG. The OCA must sign annotating the revisions, and sign or initial the review on the front cover.

8. SCG Oversight. The DUSN Security Directorate provides oversight of the SCG process to ensure they are properly completed and will review a portion of the SCGs on hand each year to ensure compliance with this policy. This may be done in conjunction with Inspector General inspections or during site assist visits.

9. Transfer of an SCG from one OCA to Another

a. Transferred SCGs must be authorized in writing by the originating OCA and the recipient OCA. The gaining OCA shall provide a copy of the written confirmation to their Service security representative and DUSN Security Directorate.

b. The gaining OCA will evaluate and, if needed, revise the SCG. If revision is required follow the procedures for developing/revising an SCG.

10. Cancellation/Declassification of an SCG

a. For all cancellations/declassifications of SCGs, follow the requirements of sections 10 and 11 of enclosure (6) of volume 1 of reference (f), and any Service issued policy. DUSN Security Directorate will be notified immediately whenever an SCG is to be cancelled using the “SCG Cancellation Letter Template.”

b. For classified elements to be declassified as a result of the SCG cancellation, the OCA shall coordinate with the DON Declassification Program Manager to ensure the DON Declassification Guide is properly updated.

ALTERNATIVE COMPENSATORY CONTROL MEASURES

1. ACCM

a. Comply with section 18 of enclosure (2) of volume 3 of reference (f) and the following specific DON implementing requirements.

b. All templates referenced in this enclosure can be found on the Information Security SharePoint.

2. Guidance for Managing ACCM

a. DON approval, oversight, management, and reporting of ACCM:

(1) The DUSN is the Security Executive executing SAO designated responsibilities for requirements in paragraph 1-6.2 of reference (ag), which includes ACCM.

(2) The DUSN (S&I) Directorate will coordinate with the SAPCO, Deputy CNO for Information Warfare, DNI (N2N6), USMC Deputy Commandant for Information, and DIRINT to ensure conflicts do not exist between classified efforts and to facilitate determination of whether classified program information may or may not require protections under SAP or SCI controls (reference (n)).

b. The ACCM sponsor is the DON OCA, per section 18f(1)(b) of enclosure (2) of volume 3 of reference (f). The OCA originally classifies information (i.e., to classify information in the first instance) at the level of or lower than the level designated by the SECNAV or DUSN for classified program information protected by ACCM. He or she may employ ACCM per requirements of section 18 of enclosure (2) of volume 3 of reference (f). The ACCM sponsor must ensure key personnel are designated for a tiered management approach to enforce ACCM within and external to his or her activity. The duties of the designated positions below can be assumed by current security staff, identified in sections 8b and 8c of enclosure (2) of volume 1 of reference (f). Additional procedures are outlined in the “ACCM Security Plan Template:”

(1) Control Officer. The ACCM control officer is designated by the ACCM sponsor and is a required position to regulate access to classified program information approved for ACCM and exercises oversight on behalf of the ACCM sponsor. Additional detailed requirements are outlined in the "ACCM Designation of Positions Template."

(2) Gatekeeper. The gatekeeper is designated by the ACCM control officer and is optional, depending on the complexity of the program (e.g., number of personnel granted access, various locations, number of activities, etc.). There can be multiple gatekeepers designated within and external to the activity to assist the ACCM control officer. He or she authorizes access to specific elements of classified program information approved for ACCM within an activity or a specific group, after need-to-know is established. Additional detailed requirements are outlined in the "ACCM Security Plan Template."

(3) Safeguard Administrator. The safeguard administrator can be designated by either the ACCM control officer or gatekeeper and is optional, depending on the complexity of the program (e.g., number of personnel granted access, various locations, number of activities, etc.). There can be multiple safeguard administrators within and external to the activity to assist the ACCM control officer or gatekeeper. He or she administers and implements the security plan within an activity or a specific group and enforces the need-to-know. Additional detailed requirements are outlined in the "ACCM Security Plan Template."

3. Waivers and Exceptions

a. When conditions exist that prevent compliance with a specific standard, or costs of compliance exceed available resources for requirements in reference (f) and this enclosure, the ACCM sponsor must submit a written request for a waiver or exception via the administrative chain-of-command to the DUSN Security Directorate using the DON tasking system using the "Waiver or Exception to Standard or Requirement Template:"

(1) Waiver. A waiver may be granted to provide temporary relief from a specific requirement pending completion of an action that will result in compliance with this manual.

(2) Exception. An exception may be granted to accommodate a long-term or permanent inability to meet a specific requirement.

b. Once received, DUSN Security Directorate will review the request. If a favorable recommendation is made it will be submitted to DUSN for approval. If the DUSN disapproves a request, it will be returned to the activity by the DUSN Security Directorate with a reason for disapproval. DUSN Security Directorate will submit for approval to the OUSD (P) those requests related to foreign government information and security arrangements for international programs.

c. Waivers and exceptions are self-cancelling at the end of the specified period. For activities having received a waiver or exception from the DUSN, that activity must submit a renewal request to the DUSN via DUSN Security Directorate not less than 30 working days prior to its expiration. For activities having received a waiver or exception from the OUSD (P), that activity must submit a renewal request to the OUSD (P) via DUSN Security Directorate not less than 60 working days prior to its expiration.

4. DON Proponents. The DUSN is the DON staff proponent for ACCM management, oversight, and reporting to the OUSD (P). These duties are executed by the DUSN Security Directorate.

5. Approval. The DUSN approves ACCM for classified information over which the DON has cognizance (i.e., DON originally classified information). The ACCM sponsor must submit specific information required in the “ACCM Request to Establish Template,” to include it’s three enclosures – (1) “ACCM Security Plan Template,” (2) SCG(s), and (3) “Data Analysis for ACCM Approval Template,” to the DUSN via the DUSN Security Directorate to initiate the approval process for use of ACCM. The approval process includes nine steps:

a. Step 1 - OCA. Does the information meet the requirements for employing ACCM in accordance with sections 18c and 18e of enclosure (2) of volume 3 of reference (f)?

(1) Yes

(a) Office of the SECNAV (DON Secretariat) and USN

1. Submit formal letter, using the “ACCM Request for Nickname Assignment Template,” to the DUSN via the DON tasking system to request the second word nickname approval with a brief description of the requirement.

2. Office of the SECNAV (DON Secretariat) and USN first word nicknames for DON ACCMs is “LIMIT.”

(b) USMC

1. Submit formal letter, using the “ACCM Request for Nickname Assignment Template,” to the DUSN via DON tasking system to request the second word nickname approval with a brief description of the requirement.

2. USMC first word nicknames for DON ACCMs is “PIVOT.”

(2) No. ACCM is not authorized.

b. Step 2 - DUSN Security Directorate. Does request comply with the requirements to establish an ACCM nickname, including requirements for selecting second word nickname assignment?

(1) Yes

(a) Office of the SECNAV (DON Secretariat) and USN. Draft and submit a written request via the DON tasking system to Office of the CNO (OPNAV N312) to validate and register the nickname.

(b) USMC. Draft and submit a written request via the DON tasking system to Deputy Commandant, Plans, Policy, Operations, and Security (DC, PP&O PS) to validate and register the nickname.

(2) No. Respond in the DON tasking system with additional guidance to the OCA on requirements to establish nickname.

c. Step 3 - OPNAV N312 and DC, PP&O PS. Register nickname and update the DON tasking system.

d. Step 4 - DUSN Security Directorate

(1) Draft formal response to OCA advising them of the nickname approval; include in the response approval does not constitute authority to use ACCM.

(2) Once signed, upload letter to DON tasking system along with additional guidance for submission of ACCM request to use package.

e. Step 5 - OCA. The OCA will:

(1) Develop a SCG, using the “SCG Format and Preparation Template,” and request an SCG ID number from DUSN Security Directorate or update an applicable existing SCG to include the ACCM-specific criteria.

(2) Develop the standard operating procedures (SOP) for the ACCM.

(3) Draft a letter of justification.

f. Step 6 - DUSN Security Directorate. Assist OCA, if requested, to ensure SCG, SOP, and justification are appropriate and accurate.

g. Step 7 - OCA. Once reviewed by DUSN Security Directorate, OCA signs SCG and SOP, and submits their formal request for use of ACCM via the DON tasking system.

h. Step 8 - DUSN Senior Director for (S&I)

(1) Determines if the request meets the requirements for approval.

(2) Forwards the request to DUSN for approval and issues formal letter of approval to the OCA via the DON tasking system. Included with the approval is the requirement for strict ACCM policy compliance.

i. Step 9 - DUSN Security Directorate. Provides a copy of the approval letter to the OUSD (P).

6. Guidance on Use. Use of ACCM must be consistent with the following:

a. The ACCM sponsor must comply with the requirements in section 18c of enclosure (2) of volume 3 of reference (f).

b. The ACCM sponsor must submit Nickname Assignment (NICKA) requests to the DUSN Security Directorate for review, registration, and approval using the "ACCM Request for Nickname Assignment Template." Nicknames have two separate words. Registration and approval of a nickname is only the first step and does not constitute establishment for the use of an ACCM. Requirements in paragraph 8 (if applicable) and 9 of this enclosure apply for subsequent steps to request and obtain approval to use ACCM for classified program information.

(1) All DON Secretariat and USN ACCM nickname first word assignments begin with "LIMIT." All USMC ACCM nickname first word assignments begin with "PIVOT." The ACCM sponsor must identify the second word assignment, per paragraph 5 of reference (i), or reference (j), as applicable.

(2) Comply with paragraph 17 of this enclosure if there is a requirement to change the ACCM nickname assignment.

c. The DUSN Security Directorate will provide written notification within 30 days to the Director of Security at OUSD (I) and the Director Special Programs at OUSD (P), once the DUSN approves ACCM use for classified program information or when an ACCM is terminated.

d. Recurrent inspections of approved ACCMs are as follows:

(1) DUSN Security Directorate will conduct annual oversight inspections of all DON approved ACCMs, based on the "ACCM Inspection Checklist," and provide the results to DUSN within 30 days after each inspection. The inspection results are also reported to the DON Sensitive Activities Review Group via the Sensitive Activities Working Group for additional oversight, per reference (ai).

(2) DUSN will provide a written report to the ACCM sponsor with the final results identifying findings, deficiencies, best practices, and recommendations within 30 days following the date of the inspection. The ACCM sponsor must submit a corrective action plan, in the event findings or

deficiencies are discovered, within 45 days of the date of the report.

(3) The ACCM sponsor will ensure annual self-inspections are conducted, using the "ACCM Inspection Checklist," for compliance with the policy guidance in section 18 of enclosure (2) of volume 3 of reference (f). Additionally, the ACCM sponsor must determine the appropriate means to inspect or collect inspection data from external activities granted access to classified program information approved to use ACCM as part of their validation of compliance with the cited policies.

7. Prohibited Security Measures. The ACCM sponsor must comply with the requirements in Section 18d of enclosure 2 of volume 3 of reference (g).

8. Prohibited Uses. The ACCM sponsor must ensure strict compliance with section 18e of enclosure (2) of volume 3 of reference (f), and obtain an exception to use ACCM for NATO or non-intelligence FGI, if applicable. The following requirements apply to obtain an exception:

a. The ACCM sponsor must clearly identify in the documentation required in paragraph 9b of this enclosure a requirement to use ACCM for NATO or non-intelligence FGI.

b. DUSN Security Directorate will coordinate with the Director, International Security Programs, Defense Technology Security Administration, OUSD (P), for action and obtain approval from the appropriate authority. Additionally, DUSN Security Directorate will submit the request for ACCM approval to the DUSN, including a copy of the exception to use ACCM for NATO or non-intelligence FGI granted by the appropriate authority.

c. The DUSN Security Directorate and the ACCM sponsor must retain a copy of the exception granted by the appropriate authority to use ACCM for NATO or non-intelligence FGI.

9. Documentation

a. DUSN must approve in writing the use of ACCM for classified program information as stated in paragraph 6 of this enclosure.

b. The ACCM sponsor must comply with the following requirements when submitting a request to DUSN to obtain approval to use ACCM for classified program information:

(1) Prior to requesting authorization to use ACCMs, formally request from OPNAVs N2N6I and N9SP/DON SAPCO written verification that SCI and SAP protections are not warranted for the classified program information.

(2) Ensure requirements in paragraph 6b of this enclosure using the "ACCM Request for NICKA Template."

(3) Ensure ACCM sponsor designation complies with the requirements in paragraph 2b of this enclosure.

(4) Ensure key personnel identified in paragraph 2b of this enclosure are designated in writing using the "ACCM Designation of Positions Template." To ensure compliance with section 18f(1)(c) of enclosure (2) of volume 3 of reference (f), subsequent changes to the designation of an ACCM Control Officer must be provided to DUSN Security Directorate, for further reporting to the Special Programs Office, OUSD (P). Additionally, the ACCM control officer, at a minimum, should be notified of any subsequent changes to the designation of gatekeepers and safeguard administrators.

(5) Using the "ACCM Request to Establish Template" to formally request approval from DUSN via DUSN Senior Director for Security to use ACCM for classified program information. The request to establish ACCM letter must include the following five enclosures: (1) "ACCM Security Plan;" (2) "ACCM Designation of Positions Template;" (3) "ACCM Data Analysis Template;" and (4) the "SCG Format and Preparation Template," for compliance with section 18b of enclosure (2) of volume 3 of reference (f).

(6) Develop the program briefing material. Distribute the security plan and SCG required documentation to be developed and submitted in paragraph 9b(5) of this enclosure and the program briefing material to all participating activities, after approval has been granted by DUSN to use ACCM.

10. Annual Reports. Per section 18g of enclosure (2) of volume 3 of reference (f), the DON must provide a report to OUSD (P) on all uses of ACCM no later than 15 December of each calendar

year. The exact format of this report will be provided annually by DUSN Security Directorate via the formal DON tasking system.

11. Sharing. DON activities approved to use ACCM must comply with the requirements in section 18h of enclosure (2) of volume 3 of reference (f) and this enclosure.

12. Contractor Access. The ACCM control officers must validate compliance with section 18i of enclosure (2) of volume 3 of reference (f) and the following:

a. Ensure each DD Form 254, "Contract Security Classification Specification," and statement of work identify the assigned ACCM nickname to which the contractor will need access in the performance of the contract.

b. Ensure the appropriate SCG and security plan for the ACCM are identified on the DD Form 254. Care must be taken to ensure identification of the security plan does not disclose the classified program information requiring ACCM.

13. Program Maintenance. The ACCM sponsor and control officer must ensure strict compliance with section 18j of enclosure (2) of volume 3 of reference (f) and the following:

a. The ACCM Control Officers, internal and external, must ensure the ACCM sponsor is provided accurate data on the number of personnel accessed.

b. When compiling the annual reporting data required in paragraph 11 of this enclosure, conduct a review of the ACCM documentation (i.e., security plan, SCG, program briefing, and training material) to ensure currency and update as required. Provide DUSN Security Directorate a copy of ACCM documentation within 10 working days of being updated.

c. Any modification to the ACCM sponsor or justification for using ACCM must be reviewed by the DUSN via DUSN Security Directorate for reassessment of continued approval.

14. Safeguarding. The ACCM sponsor must ensure strict compliance with section 18k of enclosure (2) of volume 3 of reference (f) and the requirements outlined in the security plan. Additionally, use the TS, secret, and confidential cover

sheets (i.e., SFs 703, 704, and 705, respectively, used to cover ACCM material shall be over stamped or marked with “ACCM” and the appropriate nickname).

15. Security Incidents. Participants granted access to classified program information approved to use ACCM must comply with section 18l of enclosure (2) and section 3f(1) of enclosure (6) of volume 3 of reference (f), reference (aj), and the security plan.

16. Change to Nickname. The ACCM sponsor must comply with paragraph 6b of this enclosure when there is a requirement to change the ACCM nickname for operations security reasons or in response to an actual compromise of the operation(s) associated with the current nickname, including the following:

a. Update the ACCM documentation (i.e., security plan, SCG, program briefing, and training material), prior to the effective date of the change and comply with paragraphs 13(b) and (c).

b. Disseminate the effective date for the change to all participants granted access in sufficient time to allow implementation of proper safeguards for the new nickname.

c. Provide guidance for remarking, storing, and archiving legacy classified program information under the previously assigned ACCM nickname.

17. Termination. The ACCM sponsor must notify DUSN via DUSN Security Directorate in writing, using the “ACCM Request to Terminate Template,” when use of ACCM for the classified information is no longer required; additionally, use the “ACCM Termination Checklist Template” as a guide when terminating an ACCM. DUSN Security Directorate will ensure compliance with the reporting requirement in paragraph 11, above, and provide the ACCM sponsor with an ACCM termination memorandum.

18. Transitioning to a SAP. If the DUSN and/or ACCM Sponsor identifies a potential requirement for additional protection of ACCM information using SAP controls, the DUSN and/or ACCM Sponsor shall provide, in writing, a formal recommendation and request for authorization to establish a DON SAP to the Director, DON SAPCO. If approved, responsibility for security management of the classified information will be transferred to

the Director, DON SAPCO, per references (h) through (j), (n), and (ai).

VIOLATIONS OF THIS INSTRUCTION

1. Military personnel are subject to disciplinary action under the Uniform Code of Military Justice, or criminal penalties under applicable Federal Statutes, as well as administrative sanctions, if they knowingly, willfully, or negligently violate the provisions of this instruction.

2. Civilian employees are subject to criminal penalties under applicable Federal law, as well as administrative sanctions including but not limited to removal from the Federal service, if they knowingly, willfully, or negligently violate the provisions of this instruction.

RECORDS MANAGEMENT

1. Records created as a result of this instruction, regardless of format or media, must be maintained and dispositioned according to the records disposition schedules found on the DRMD portal page: https://portal.secnav.navy.mil/orgs/DUSNM/DONAA/DRM/SitePages/Home.aspx.

2. For questions concerning the management of records related to this instruction or the records disposition schedules, please contact your local Records Manager or the DRMD Program Office.

FORMS AND REPORTS

1. Forms. DD Form 254, DoD Contract Security Classification Specification, and DD Form 2024, DoD Security Classification Guide Data Elements, are available from the official DoD website for DoD Forms, https://www.esd.whs.mil/directives/forms/.

2. Reports. The reporting requirements contained in enclosure (2), paragraphs 12j, 13d, 19i, 20r, and enclosure (5) paragraphs 5 and 10 are exempt from information collection control, per reference (ak), Part IV, paragraphs 7c.