CHAIRMAN OF THE JOINT CHIEFS OF STAFF INSTRUCTION

J-3	CJCSI 3213.01D
DISTRIBUTION: A, B, C, S	7 May 2012

JOINT OPERATIONS SECURITY

References: See Enclosure C

1. Purpose. To provide CJCS policy and guidance for planning and executing operations security (OPSEC) in support of joint military operations, activities, plans, training, exercises, and capabilities.

2. Superseded/Cancelled. CJCSI 3213.01C, 17 July 2008, "Joint Operations Security," is hereby superseded.

3. Applicability. This instruction applies to the Joint Staff, Combatant Commands, Services, Combat Support Agencies, and joint activities reporting to the Chairman of the Joint Chiefs of Staff (hereinafter referred to collectively as the DoD Components").

4. Policy. Applicable organizations will plan and execute OPSEC operations, activities, plans, training, exercises, and capabilities in accordance with this instruction. See Enclosure A.

5. Definitions. See Glossary.

6. Responsibilities. See Enclosure B.

7. Summary of Changes. This revision of CJCSI 3213.01:

a. Includes OPSEC considerations in contracting, in the review procedures prior to public release of information, and during Freedom of Information Act (FOIA) requests.

b. Broadens the scope of OPSEC training and expands the audience to include DoD family members and others.

c. Discusses the relationship between military deception (MILDEC) and OPSEC.

d. Provides guidance on social media, OPSEC enforcement, and funding for OPSEC programs.

e. Discusses the requirement for a full-time OPSEC program manager at the command level and expands the responsibilities.

f. Includes specific duties for the OPSEC planner.

g. Defines responsibilities for the Joint Information Operations Warfare Center (JIOWC); Commander, USSOCOM; and all DoD Component personnel.

h. Shifts joint OPSEC oversight responsibility from Commander, USSTRATCOM, to the Chairman.

i. Includes items for inclusion in critical information lists.

8. Releasability. This instruction is approved for public release; distribution is unlimited. DOD components (to include the Combatant Commands), other Federal agencies, and the public may obtain copies of this instruction through the Internet from the CJCS Directives Home Page--http://www.dtic.mil/cjcs_directives.

9. Effective Date. This instruction is effective upon receipt.

WILLIAM E. GORTNEY
VADM, USN
Director, Joint Staff

Enclosures:

A — Policy
B —Responsibilities
C —References
GL —Glossary

DISTRIBUTION

Distribution A, B, and C plus the following:

	Copies
Under Secretary of Defense for Intelligence	2
Under Secretary of Defense for Policy	2
Director, Joint Interoperability Test Command	2
Commandant, Joint Forces Staff College	2
President, National Defense University	2
Director, Joint Navigation Warfare Center	2
Director, Joint Information Operations Warfare Command	2
Director, Joint Warfare Analysis Center	2
Director, Joint COMSEC Monitoring Activity	2
Commander, Joint Personnel Recovery Agency	2
Director, Joint Center for International Security Force Assistance	2

(INTENTIONALLY BLANK)

TABLE OF CONTENTS

Page

ENCLOSURE A -- POLICY

ENCLOSURE B -- RESPONSIBILITIES

(INTENTIONALLY BLANK)

ENCLOSURE A

POLICY

1. The Need for OPSEC

a. Joint operations are complex and possess vast amounts of information that an adversary wants to obtain. Protecting this information is vital to mission success and is accomplished through OPSEC planning.

b. OPSEC supports joint operations and is an integral part of operations, activities, plans, exercises, training, and capabilities. OPSEC supports information operations (IO), MILDEC, and security programs.

c. Security programs and procedures already exist to protect classified information. Sensitive unclassified (critical) information and certain detectable activities (indicators) can reveal friendly intentions and must be protected as well. Such information or indicators may assist those seeking to neutralize or exploit friendly operations, activities, plans, exercises, and capabilities. Application of OPSEC promotes operational effectiveness by helping to prevent the inadvertent disclosure of sensitive unclassified information or intentions.

d. As we have learned from the *Manchester Document*, a terrorist handbook discovered during a raid of an Al Qaida safe house in Manchester, England, in 2000, as much as 80 percent of the information collected by terrorists includes publicly available information from sources such as the news media, internet-based capabilities (including social media), and observable activities of U.S. Military Forces. Adversaries often collect what appears to be insignificant unclassified data. However, when this data is aggregated with other pieces of information, it may provide a comprehensive view of friendly activities and intent that the adversary can use to act against friendly forces. OPSEC is critical to mitigating open source vulnerabilities and prevents data aggregation and disclosure of sensitive critical or classified information.

e. Protection of critical information is essential to mission accomplishment; however, it is becoming increasingly difficult to protect, due to the speed and availability of new technologies that allow information to be shared quickly and effortlessly from anywhere in the world. Continual evaluation of our OPSEC posture is needed to protect U.S. forces and operations from this and other evolving threats and associated vulnerabilities.

f. The purpose of OPSEC is to enable operations and activities through the use of essential secrecy, assuring the greatest opportunity for U.S., coalition, and combined forces to maintain an operational advantage over adversaries, competitors, and others. As a capability, OPSEC protects plans, missions, and lives by reducing the vulnerability of U.S., coalition, and combined forces from successful adversary exploitation of critical information. OPSEC applies across the entire range of military operations and is required:

(1) For any operation or activity, such as those that relate to the equipping, preparation, deployment, sustainment, or post-execution of U.S. Military Forces in time of peace, crisis, or war.

(2) For the protection of the critical information contained in operation plans in concept format (CONPLANs), operation plans (OPLANs), operation orders, and supporting plans and orders.

2. OPSEC and Operational Effectiveness

a. OPSEC contributes directly to operational advantage by increasing mission effectiveness and protecting the unit's critical but sensitive information. A surprised adversary—or an adversary that has been unable to consolidate the necessary information in a timely manner to hinder or render friendly missions ineffective—will likely be defeated more quickly, with fewer friendly losses, than one who is prepared and well-informed.

b. To make a maximum contribution to operational effectiveness, there must be a balance between what information must be denied to adversaries, competitors, and others, and what must be known to friendly personnel. Application of excessive countermeasures may hinder coordination, synchronization, execution, and assessments of required activities. This limits the ability for the actor to gain or maintain an operational advantage (surprise) due to restriction on information dissemination.

c. The OPSEC process recognizes that risk is inherent in all military activities. The determination of the appropriate level of protection versus operational needs requires an assessment of those risks. The use of the OPSEC process will assist commanders and operations planners in determining the specific risk to mission, information, personnel, and facilities. Determining the balance between OPSEC countermeasures and operational needs is the commander's decision.

d. OPSEC is a force multiplier that can maximize operational effectiveness by saving lives and resources when integrated into operations, activities, plans, exercises, training, and capabilities.

3. OPSEC, Security, and Counterintelligence

a. OPSEC is an operations function and requires close integration with the various security programs intended to protect information, personnel, and resources. OPSEC as a capability employs a process that identifies actions to deny, disrupt, or deceive an adversary's ability to collect critical information and observable indicators that are sensitive, but unclassified. Proper employment of the OPSEC process will minimize the conflicts throughout the operations process. Each operation is to be analyzed to determine its vulnerabilities and identify potential risks to mission success. The commander must then determine what measures will be taken to counter the threat or mitigate vulnerabilities.

b. Establishing and maintaining essential secrecy by DoD personnel is imperative to gain operational advantage over adversaries. Essential secrecy is the condition achieved by denying critical information to adversaries through the combined efforts of traditional security programs and the OPSEC process.

(1) Traditional security programs are designed to protect personnel, information, and resources. These security programs include, but are not limited to: physical, information, industrial, communications, research and technology protection, and information assurance (IA).

(2) OPSEC considers security requirements during the planning of operations or activities. Coordination and synchronization by all participants during planning and execution will ensure security measures are not overlooked or hindered. Planners employ the OPSEC process to identify and control indicators, minimize vulnerabilities and signatures, and protect friendly critical information.

c. Counterintelligence will support both OPSEC and security programs and helps achieve essential secrecy by identifying threats and their tactics, techniques, and procedures (TTPs), which can be used to assess OPSEC countermeasures.

4. <u>OPSEC and Information Operations (IO)</u>. IO is the integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own. IO requires the identification of information related-capabilities, such as OPSEC, that are most likely to achieve the Combatant Commander's desired effects or prevent an adversary from achieving its goals. OPSEC is an operations function that, when effectively applied and fully integrated into the life-cycle of military operations, provides, along with other IO core capabilities, a fully integrated warfighting/peacetime capability, as well as other information-related capabilities. The OPSEC process is continuous and significantly contributes to the following IO functions:

a. Deter, disrupt, degrade, and deceive an adversary, thereby disrupting the enemy's ability to effectively command while preserving unity of effort. OPSEC is integral to degrading the adversary's understanding of a given situation by denying or otherwise interrupting the information they need to counter our efforts.

b. Protect plans and prevent the collection of critical information and observable indicators by enemy forces, thereby allowing U.S. Military Forces to mass their effects to maximum advantage while the adversary expends resources to little effect.

c. Degrade the adversarial command and control process, thereby crippling the adversary's ability to direct and organize while preserving effective command and control of U.S. Military Forces.

d. OPSEC and MILDEC are mutually supportive and as such must be fully integrated at all levels in order to maximize effective support to friendly operations, activities, plans, and capabilities. MILDEC supports OPSEC by providing potential countermeasure development, approval, and implementation support. OPSEC supports MILDEC by utilizing the OPSEC process to identify risks which can potentially be mitigated by MILDEC.

(1) Deception in Support of OPSEC (DISO). A DISO is a military deception activity that protects friendly operations, personnel, programs, plans, capabilities, equipment, and other assets against foreign intelligence security services (FISS) collection. The intent of a DISO is to create multiple false indicators to confuse or make friendly force intentions harder to interpret by FISS and other adversary (such as violent extremist organization (VEO) or paramilitary) intelligence gathering apparatus, limiting the ability of FISS to collect accurate intelligence on friendly forces. DISOs are general in nature; they are not specifically targeted against particular adversary military, paramilitary, or VEO decision-makers, but are instead used to protect friendly operations and forces by obfuscating friendly capabilities, intent, or vulnerabilities.

(2) OPSEC planners and program managers have a supporting relationship to MILDEC planners regarding the development, approval, and implementation of DISOs. DISOs will not be planned or executed without coordination with the command MILDEC Officer. For additional information, see reference h.

5. The OPSEC Process. OPSEC is a standardized, continuous, and iterative process that is applicable to all military operations and activities (to include support activities), as these efforts often provide indicators to the adversary about our current and future military operations and activities. The OPSEC

process ensures countermeasures address all significant aspects of the particular situation and are balanced against operational requirements. The elements of the process (reference c) are:

a. Identification of critical information.

b. Analysis of threats.

c. Analysis of vulnerabilities.

d. Assessment of risks.

e. Application of appropriate OPSEC countermeasures.

6. OPSEC Programs. Commanders and heads of DoD Components are required to establish, resource, and maintain formal OPSEC programs. The primary purpose of a formal OPSEC program is to support the commander by ensuring OPSEC is exercised to enable operations or activities through the denial of critical information or observable indicators to adversaries. OPSEC programs consist of the manning, training, and equipping functions necessary to enable the conduct of OPSEC planning and execution support to joint operations, activities, plans, exercises, training, and capabilities. OPSEC programs promote an understanding and awareness of OPSEC among all members (military, civilian, and contractor) of the command or agency. OPSEC awareness should be extended to others (such as external agencies, allies, coalition partners, and DoD family members) who have a need for access to critical information, to ensure they understand the threat and the value of the information they are receiving. To be effective, an OPSEC program must have the following features:

a. Command Involvement. OPSEC is a commander's responsibility and success or failure is due in part to the active involvement and support. The commander must provide OPSEC policy and planning guidance early in the program development process, to include approving the list of critical information and identifying activities that must be protected. The commander may delegate program management, planning, and its execution to subordinates, however, the commander retains the responsibility to determine the acceptable level of risk and which OPSEC countermeasures to implement. OPSEC must be added as a key compliance item for inspections at all levels of command.

b. Critical Information List. When identifying critical information, DoD Components must consider information pertaining to critical infrastructures, facilities, and equipment; acquisition of products and services; and Research, Development, Test, and Evaluation (RDT&E) efforts, in addition to information related to traditional military operations, functions, and activities. In developing the list, OPSEC personnel should review the organization's Essential Elements of Friendly Information to ensure they are mutually supportive (reference d).

c. Funding. DoD Components will ensure dedicated manpower, funding, and resources are available to implement and sustain the OPSEC program. They will account and plan for resources in accordance with the Planning, Programming, Budget, and Execution System (PPBES) by identifying funding requirements and resource allocations in accordance with their components Program of Memoranda cycle requirements. Commanders must consider OPSEC funding during the Integrated Priority List (IPL) process.

d. Review for Public Release. OPSEC should not be used as an excuse to deny non-critical information to the public. DoD Components shall implement review processes prior to public release to assess the potential impact of the release. Information should be looked at alone but also in aggregation with other information to protect against unintentional disclosure of critical information.

e. Freedom of Information Act Considerations. FOIA, codified as title 5, United States Code, section 552, is a law that provides the public access to federal agency records. DoD Components will disclose information requested under FOIA, unless the information is identified as one of the nine FOIA exemptions that were established to preclude the disclosure of information that requires protection. DoD Components shall establish policies that formulate internal FOIA procedures to ensure both FOIA and OPSEC objectives are met.

f. Contracting Considerations. DoD Components will ensure that contract requirements properly reflect OPSEC responsibilities, to include protecting critical information both at rest and in transit in accordance with contracting guidance and that those responsibilities are included in contracts when applicable. DoD Components shall ensure that contractor personnel (to include off-site personnel) who have access to DoD critical information receive appropriate and timely OPSEC awareness training.

g. Integration. In order to be effective, the OPSEC process must be integrated into the planning and execution of all military operations, functions, and activities. As part of planning, OPSEC must be incorporated early in the conceptual phase of the planning process. Critical information must be identified for subordinate and supporting commands and specific guidance on the execution of OPSEC countermeasures provided to them. Defense support to public diplomacy, public affairs, and civil military operations are activities related to IO. These planners must be kept informed of that guidance and critical information for incorporation into their planning and operations.

(1) OPSEC must be coordinated and synchronized with other information-related capabilities to achieve the commanders' intent. OPSEC is particularly important for MILDEC and Military Information Support Operations. Cross-command and interagency support and coordination during all phases of the OPSEC process enhance program effectiveness.

(2) Coordination is particularly vital for activities involving multiple commands and agencies. Because of the importance of coalition warfare to U.S. national strategy, allies and partners will be encouraged to implement their own OPSEC programs or adopt U.S. joint OPSEC concepts. Close coordination is required with intelligence organizations to identify potential adversaries and their intelligence collection capabilities and to determine the effectiveness of OPSEC measures taken.

h. OPSEC and Social Media. Social media is a popular and effective communications tool that presents a unique challenge to commanders. The speed, ease of use, and proliferation of social media has changed the operational environment and introduced new vulnerabilities that create a threat to DoD missions and personnel. Not only must personnel be vigilant when using social media to ensure they do not disclose critical information; but planners must be aware that an indicator observed by one individual may be shared via social media, instantaneously with millions of others around the world. All DoD Components must review and update their OPSEC programs to ensure social media policies, plans, education and training, and appropriate countermeasures are in place to reduce vulnerabilities and indicators, thereby mitigating risk.

i. Training and Education. Training and education programs ensure all personnel understand their role in OPSEC, are aware of any intelligence threats to the command, know the command's critical information, and understand how to implement directed OPSEC countermeasures. OPSEC training programs must be mission-related and tailored for specific operational functions. All personnel must understand that implementing OPSEC countermeasures to protect critical information is command and individual responsibility.

(1) The general workforce (to include contractors) shall receive OPSEC awareness training upon initial entry to duty and annually thereafter. OPSEC training must be incorporated into accession programs for civilian and military members, to include basic training and commissioning programs.

(2) OPSEC program managers, coordinators, planners, IO professionals, intelligence personnel supporting OPSEC planning, PA personnel, contracting personnel, personnel responsible for the review and

approval of information intended for public release, and deploying members, as a minimum, shall receive additional OPSEC training specific to their duties.

(3) OPSEC training and education must be included in military education at all levels. Curriculum managers will ensure training and education programs are accredited to meet joint standards. Additional training that is specific to unit or organizational function or mission will be considered internal training to that organization. Personnel may receive training by either an OPSEC Program Manager, OPSEC Planner, or both.

(4) DoD family members and others who require access to critical information shall receive OPSEC awareness instruction and support, consistent with reference i.

(5) The following organizations provide OPSEC training for their specific areas of responsibility:

(a) The National Security Agency, through the Interagency OPSEC Support Staff (IOSS), conducts interagency OPSEC training (reference a).

(b) JIOWC/Joint OPSEC Support Element (JOSE), through the Chairman, provides training to Combatant Commanders and Joint Force Headquarters (reference b).

(c) USSOCOM OPSEC support element provides training to its command and subordinates.

(d) Service OPSEC support elements provide training to their corresponding Services (reference b).

j. OPSEC Enforcement. Commanders shall ensure a process is in place to report disclosures of critical information so mitigating actions can be implemented. They shall ensure personnel are aware that failure to follow OPSEC guidance can result in disciplinary action; and will hold accountable personnel who violate OPSEC policies.

k. Annual Reviews. Annual reviews to determine the status of a command's OPSEC program are necessary to gauge program success and identify improvements. Heads of DoD components shall submit annual reviews of their OPSEC programs to the Under Secretary of Defense for Intelligence (see reference b).

l. Evaluation of OPSEC Programs. Evaluation of the organization's program can be made by assessing the program for completeness and by surveying the organization's OPSEC posture to determine effectiveness.

Evaluations from both a friendly and adversarial perspective provide insight into the command's OPSEC posture and allow commanders to focus on identified vulnerabilities. Upon request, the IOSS, JIOWC/JOSE, and USSOCOM and Service OPSEC support elements can conduct external surveys for their corresponding areas of responsibility.

(1) OPSEC Assessments. This term refers to an evaluative process conducted annually on an organization, operation, activity, exercise, or support function to determine if sufficient countermeasures are in place to protect critical information. An OPSEC assessment may include program reviews, inspector general inspections, or higher headquarters assessments that specifically address OPSEC. The OPSEC assessment team should be composed of the OPSEC Program Officer and representatives from throughout the organization.

(2) OPSEC Surveys

(a) A survey is the application of the OPSEC methodology by a team of experts to conduct a detailed analysis of activities associated with a specific organization, operation, activity, exercise, or support function by employing the known collection capabilities of potential adversaries. This evaluation should focus on the agency's ability to adequately protect critical information from adversary intelligence exploitation during planning, preparation, execution, and post-execution phases of any operation or program.

(b) Surveys should be done by an external organization emulating TTPs. The term "survey" implies an integrated team of experts from multiple disciplines who are providing analytic support (such as telecommunications monitoring, radio frequency monitoring, network and computer assessment, and open-source research) to an organization other than their own. Threat-based comprehensive OPSEC surveys are conducted, at a minimum, every 3 years. Automated risk analysis tools should be leveraged to aid in the identification of vulnerabilities and applicable countermeasures.

(c) Activities that warrant OPSEC surveys include, but are not limited to: RDT&E; acquisitions; treaty verification; nonproliferation protocols; international agreements; force protection operations; special access programs; and activities that prepare, sustain, or employ U.S. Military Forces over the range of military operations.

(d) DoD components shall prioritize OPSEC survey requirements and outline procedures for scoping and requesting OPSEC survey support from the appropriate OPSEC support element.

7. OPSEC Program Managers

a. The OPSEC program manager is responsible for advising the commander on all OPSEC-related matters and for the day-to-day management of the organization's program. The position requires OPSEC Program Manager's training and a security clearance (SECRET as a minimum), appropriate to the mission and function of the organization. OPSEC training may be obtained through the IOSS, JIOWC/JOSE, USSOCOM OPSEC support element, or corresponding Service OPSEC support element.

b. The OPSEC program manager shall:

(1) Complete OPSEC Analysis and Program Management or equivalent course within 90 days of appointment.

(2) Advise the commander on OPSEC matters.

(3) Develop and maintain the organization's OPSEC program, to include drafting the organization's policy and guidance documents for the commander's approval and signature.

(4) Identify critical information; review and update it at least annually or as missions change; and distribute it within the organization to the appropriate personnel.

(5) Conduct or coordinate organizational OPSEC education and awareness training for all DoD personnel and specialized functions.

(6) Coordinate the conduct of OPSEC assessments and surveys.

(7) Conduct the organization's annual OPSEC review.

(8) Develop and maintain an organizational OPSEC continuity binder with applicable documents. The continuity binder may be hardcopy or softcopy (electronic), and must be accessible for historical purposes.

(9) Coordinate appropriate intelligence and counterintelligence support.

(10) Coordinate with security program managers, Anti-terrorism/Force Protection (AT/FP), and Critical Infrastructure Protection (CIP) planners.

(11) Coordinate development and integration of OPSEC into IO and related capabilities.

(12) Coordinate with contracting personnel to ensure DoD contract requirements properly reflect OPSEC responsibilities and that those responsibilities are included in contracts when applicable.

(13) Establish an OPSEC Working Group, to include members from other functional areas, including, but not limited to: security, AT/FP, intelligence, CIP, PA, IA, FOIA POC's, contracting, and family support groups.

(14) Ensure procedures are in place to control critical information and indicators.

(15) Coordinate with PA and others who share responsibility for the release of information to ensure a rigorous review policy is in place prior to release of unclassified information, to include the review of photos (including background details) and associated data, such as information identifying when and where the photo was taken.

(16) Provide OPSEC funding requirements for inclusion in the PPBES and IPL processes.

(17) Ensure OPSEC is addressed in operational orders and plans.

8. OPSEC Planners

a. Trained OPSEC planners should be used to conduct operational planning ensuring OPSEC is integrated throughout the planning process. In circumstances involving particularly complex operations, or operations requiring extraordinary security, it may be necessary to have dedicated OPSEC planners or create dedicated planning groups. When the planning level of effort is minimal or an OPSEC planner is not available, the OPSEC planning function may be performed by an OPSEC representative, such as an OPSEC program manager trained in planning, or a military planner trained in OPSEC.

b. The OPSEC planner shall:

(1) Complete OPSEC Analysis and Program Management or equivalent course and OPSEC for Planners specific training that is approved and certified by the Joint Staff.

(2) Provide OPSEC planning in line with the organization's OPSEC programs and policies.

(3) Participate early in the planning process to provide OPSEC guidance to protect the plan as well as the planning process.

(4) Develop OPSEC documents to be included in all plans.

(5) Coordinate with the intelligence providers to formulate a threat collection assessment.

(6) Ensure the development of the critical information lists for assigned missions or operations within a designated Area of Responsibility.

(7) Conduct an OPSEC analysis for each phase of the plan; evaluate each course of action against the commander's acceptable level of risk.

(8) Assist in the development and integration of OPSEC countermeasures into the plan to reduce vulnerabilities and indicators.

(9) Coordinate the development and integration of OPSEC into information-related capabilities.

(10) Coordinate planning effort with the organization's OPSEC program.

(11) Coordinate survey or assessment as necessary to identify vulnerabilities during operational planning and execution.

ENCLOSURE B

RESPONSIBILITIES

1. Chairman of the Joint Chiefs of Staff

a. As the joint proponent for OPSEC, provide OPSEC management oversight and oversee the operational integration of OPSEC across the Combatant Commands.

b. Advise the Secretary of Defense concerning OPSEC support to the Combatant Commands.

c. Evaluate and oversee joint OPSEC training to ensure Combatant Command requirements are met satisfactorily within the joint training system, and meet the requirements of a professionally trained and educated OPSEC capability as part of IO force development.

d. Establish and maintain a JOSE to provide OPSEC training, program review, surveys, and planning and exercise support to the Combatant Commanders and their subordinate joint force commands (reference b).

e. Provide joint OPSEC policy, doctrine, and TTPs.

f. Provide guidance to Combatant Commanders for the annual review and evaluation of their OPSEC programs.

g. Provide procedures for OPSEC planning in the Joint Operations Planning and Execution System.

h. Ensure OPSEC surveys are conducted and implemented during CJCS exercises.

2. Director for Operations (J-3), Joint Staff

a. Execute primary Joint Staff responsibility for OPSEC policy.

b. Designate OPSEC staff positions for the Joint Staff.

c. Serve as the joint OPSEC proponent coordinating with the Office of the Secretary of Defense and other agencies, as required, to advocate for and execute OPSEC programs.

d. Provide guidance for input into the Joint Staff Lessons Learned Information System data base to support OPSEC planning and training.

e. Coordinate with J-5, Joint Staff, for review of OPSEC annexes to OPLANs and CONPLANs.

f. Coordinate with J-7, Joint Staff, for inclusion of OPSEC guidance in the annual Chairman's Joint Training Guidance, and inclusion as a high interest training issue.

g. Establish OPSEC Executive Groups (OEG), as necessary, to include an OPSEC training consortium composed of members of the Joint Staff, Services, and appropriate agencies, to address specific OPSEC issues related to OPSEC programs that involve multiple commands, agencies, allied, coalition and partner nations.

3. <u>Joint Information Operations Warfare Center</u>

a. Establish and maintain the JOSE to provide OPSEC training, program review, surveys, and planning and exercise support to the Combatant Commanders and their subordinate joint force commands.

b. As the joint OPSEC subject matter experts, develop and provide the joint community with OPSEC best practices, lessons learned, TTPs, training curriculum, training, and awareness products.

c. Advise and assist in the development of OPSEC policy and doctrine.

d. Prioritize, coordinate, and integrate joint OPSEC requirements and capabilities.

e. Prepare the CJCS input to the Annual OPSEC Report submitted to USD(I).

f. Is authorized during the conduct of surveys to simulate or replicate adversarial, non-disruptive TTPs to evaluate OPSEC programs and plans. These TTPS may include, but are not limited to: observation, aggressor operations, open source collection, and social engineering.

g. Assist and advise the J-3, Joint Staff, on joint OPSEC training and OPSEC force development.

4. <u>Service Chiefs</u>

a. Provide Service OPSEC policy, doctrine, and planning procedures consistent with joint OPSEC policy, doctrine, and guidance.

b. Provide for OPSEC-related training of all Service members and family members with access to critical information, starting with basic training and commissioning programs. Ensure deploying personnel receive additional training on the development of TTPs upon real-world scenarios and their deployment locations, to decrease vulnerabilities and reduce indicators. Educate and inform family members with access to critical information about OPSEC.

c. Designate a full-time OPSEC program manager in the Service headquarters.

d. Designate representatives to Joint Staff OEGs, when required.

e. Provide OPSEC lessons learned to the J-3, Joint Staff, for inclusion in the JLLIS data base.

f. Provide to J-3, Joint Staff, copies of all current Service OPSEC program directives and/or policy implementation documents.

5. Combatant Commanders

a. Designate, and appoint in writing, a full-time OPSEC program manager in the command headquarters. Ensure OPSEC program managers are appointed at all subordinate units and joint force headquarters.

b. Provide OPSEC guidance for all command operations, exercises, and other joint activities of the command.

c. Integrate OPSEC planning into all contingency planning and operations in accordance with applicable directives and instruction. Plan for and execute OPSEC countermeasures in support of assigned missions during peacetime, crisis, and war.

d. Provide OPSEC guidance and identify command critical information to all supporting Combatant Commands, Services, other agencies, and appropriate PA offices.

e. Coordinate OPSEC countermeasures and their execution with JIOWC/JOSE for those activities that cross command boundaries. Report any unresolved issues to J-3, Joint Staff, for assistance.

f. Conduct annual OPSEC reviews and OPSEC evaluations (self-assessment annually and external survey every 3 years) in support of command operations. Identify areas requiring additional CJCS guidance, assistance, or clarification to the J-3, Joint Staff.

g. Provide OPSEC lessons learned to the J-3, Joint Staff, for inclusion in the JLLIS database.

h. Provide to J-3, Joint Staff, copies of all current command OPSEC program directives and/or policy implementation documents.

i. Identify OPSEC requirements and ensure resources are available to implement the program.

j. Notify the J-3, Joint Staff, of OPSEC requirements.

k. Complete the DoD Annual OPSEC report for the Combatant Command headquarters and subordinate joint commands IAW published guidance. Do not report Service elements which are reported through Service channels.

6. Commander, U.S. Special Operations Command

a. Establish and maintain an OPSEC support element to provide the command and its subordinates with program development, planning, training, assessment, survey, and readiness training tailored to unique special operations mission.

b. As a force provider for special operations forces, liaise with Geographic Combatant Commands and the Joint OPSEC Support Element to ensure preparedness of theater special operations commands.

7. Director, Defense Intelligence Agency

a. Establish and maintain an OPSEC training program for DIA civilian and military personnel and attendees at the Defense Intelligence College.

b. Appoint, in writing, an agency OPSEC program manager.

c. Designate representatives to Joint Staff OEGs, as required.

d. Identify, review, and validate DIA and other DoD threat assessment documents for Joint Staff use.

e. Conduct analysis of the foreign intelligence collection threat for required nations and organizations for use in OPSEC planning and for monitoring the effectiveness of implemented OPSEC countermeasures. Provide intelligence and counterintelligence thread analysis results/support to DoD Components.

8. Director, National Security Agency. In accordance with references a and b, shall, as the Federal Executive Agency for interagency OPSEC:

a. Maintain an IOSS to assist Executive Departments and agencies as needed.

b. Assist DoD components in establishing OPSEC programs and providing OPSEC services as requested.

c. Provide interagency OPSEC training and awareness courses and products.

d. Designate representatives to Joint Staff OEGs, as required.

e. Collaborate with the heads of the DoD components by providing:

(1) Technical OPSEC survey support to DoD components to assist them in identifying their OPSEC vulnerabilities.

(2) Recommendations relating to doctrine, methods, and procedures to minimize those vulnerabilities, when requested.

(3) Communications and computer security support for OPSEC surveys.

(4) Signals Intelligence support for OPSEC threat development.

(5) COMSEC monitoring services to DoD elements through the Joint COMSEC Monitoring Activity.

9. Heads of Other Defense Agencies and Joint Activities

a. Designate an agency or joint OPSEC program manager.

b. Coordinate OPSEC programs and activities with commands and other agencies, as required.

c. Provide representatives to OEGs, as required.

10. All DoD Component Personnel

a. Complete all required initial, annual, and specialized OPSEC training.

b. Protect critical information, regardless of format, from disclosure at all times.

c. Utilize encryption techniques to protect critical information both at rest on and in-transit over unclassified networks. Encrypt all e-mail messages containing critical information, OPSEC indicators, and other sensitive information.

d. Ensure all immediate family members (and extended family) are aware of the importance of protecting critical information and know how to protect critical information to which they require access.

e. Follow the organization's public release review process to prevent unintentional disclosure of critical information.

f. Report any suspected OPSEC disclosures or concerns to the OPSEC program manager and the Chain of Command.

g. Understand that failure to follow OPSEC guidance can result in administrative or disciplinary action.

ENCLOSURE C

REFERENCES

a. National Security Decision Directive Number 298, 22 January 1988, "National Operations Security Program."

b. DoD Directive 5205.02, 6 March 2006, "DoD Operations Security (OPSEC) Program."

c. DoD Manual 5205.02M, 3 November 2008, "DoD Operations Security (OPSEC) Program Manual."

d. Joint Pub 3-13.3, 4 January 2012, "Operations Security."

e. Joint Pub 1, 20 March 2009, "Doctrine for the Armed Forces of the United States."

f. Joint Pub 1-02, 8 November 2010, as amended through 15 October 2011, "Department of Defense Dictionary of Military and Associated Terms."

g. OSD memorandum, 25 January, 2011, "Strategic Communication in the DoD."

h. CJCSI 3211.01E, 25 October, 2010, "Joint Policy for Military Deception."

i. DoD Instruction 1342.22, 30 December 1992, "Family Centers."

(INTENTIONALLY BLANK)

GLOSSARY

Unless otherwise stated, the terms and definitions contained in this glossary are for the purposes of this instruction only.

counterintelligence. Information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons or their agents, or international terrorist organizations or activities. Also called CI. (JP 1-02. SOURCE: JP 2-01.2)

critical information. Specific facts about friendly intentions, capabilities, and activities vitally needed by adversaries for them to plan and act effectively so as to guarantee failure or unacceptable consequences for friendly mission accomplishment. (JP 1-02. SOURCE: JP 2-0)

essential secrecy. The condition achieved from the denial of critical information to adversaries through the combined efforts of traditional security programs and the operations security process. Upon approval of this document, this term and definition are proposed for addition to JP 1-02.

information operations. The integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt or usurp adversarial human and potential adversaries while protecting our own. Also called IO. (JP 1-02. SOURCE: SecDef memorandum 12401-10)

military deception. Actions executed to deliberately mislead adversary military, paramilitary, or violent extremist organization decision makers, thereby causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly mission. Also called MILDEC. (JP 1-02. SOURCE: JP 3-13.4)

operations security. A process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities. Also called OPSEC. (JP 1-02. SOURCE: JP 3-13.3)

operations security assessment. An evaluative process, usually exercise, or support function to determine the likelihood that critical information can be protected from the adversary's intelligence Also called OPSEC assessment. (JP 1-02. SOURCE: JP 3-13.3) operations security indicators. Friendly detectable actions and open-source information that can be interpreted or pieced together by an adversary to derive critical information. (JP 1-02, SOURCE: JP 3-13.3)

operations security planner. A functional expert trained and qualified to plan and execute operations security. Also called OPSEC planner. Upon approval of this document, this term and definition are proposed for addition to JP 1-02.

operations security Program Manager. A full-time appointee or primary representative assigned to develop and manage an operations security program. Also called OPSEC Program Manager. Upon approval of this document, this term and definition are proposed for addition to JP 1-02.

operations security survey. A collection effort by a team of subject matter experts to reproduce the intelligence image projected by a specific operation or function simulating hostile intelligence process. (JP 1-02, SOURCE: JP 3-13.3)