DEPARTMENT OF THE NAVY
BUREAU OF MEDICINE AND SURGERY
7700 ARLINGTON BOULEVARD
FALLS CHURCH VA 22042

BUMEDINST 3070.1A
BUMED-N4
8 Jul 2024

BUMED INSTRUCTION 3070.1A

From: Chief, Bureau of Medicine and Surgery

Subj: NAVY MEDICINE OPERATIONS SECURITY PROGRAM

Ref: (a) OPNAVINST 3432.1A
(b) DoD Instruction 5200.48 of 6 March 2020
(c) DoD Manual 5200.01, Volumes 1 through 3, DoD Information Security Program, 24 February 2012
(d) DoD Manual 5205.02, DoD Operations Security (OPSEC) Program Manual, 29 October 2020
(e) SECNAVINST 3070.2A
(f) DoD Directive 5205.02E of 20 June 2012
(g) NTTP 3-13.3

Encl: (1) Navy Medicine Baseline Critical Information and Indicators List
(2) Operations Security Training
(3) Sample Operations Security Program Manager Waiver
(4) Operations Security Working Group
(5) Operations Security in Contracts

1. Purpose. To establish policy, identify procedures, provide guidance, and assign responsibilities for implementing and managing the Navy Medicine (NAVMED) Operations Security (OPSEC) Program, per references (a) through (g) and enclosures (1) through (5).

2. Cancellation. BUMEDINST 3070.1.

3. Scope and Applicability. This instruction is applicable to all military, civilian, Intergovernmental Personnel Act (IPA), and contractor and subcontractor personnel, hereafter known collectively as contractor personnel, in all budget submitting office (BSO) 18 activities.

4. Background. OPSEC is critical to the success of NAVMED activities. The Department of Defense (DoD), Chief of Naval Operations and Secretary of the Navy (SECNAV) has reaffirmed all units must follow OPSEC practices in their daily application of military operations. The practice of OPSEC enables mission success by preventing inadvertent compromise of sensitive or unclassified activities, capabilities, or intentions at the strategic, operational, and tactical levels. The OPSEC cycle provides commanders with the ability to identify critical information (CI), current vulnerabilities, risks due to its vulnerabilities, and countermeasure decision criteria to mitigate those risks.

a. OPSEC is not intended to be a replacement for traditional security programs that are designed to protect classified information. OPSEC is intended to deny adversaries publicly available indicators of sensitive or unclassified activities, capabilities, or intentions.

b. The potential for exploitation of open-source material, including internet, media, and other generally unclassified but sensitive information significantly challenges the ability to provide adequate force protection as well as the conduct of other sensitive or classified activities. As a result, OPSEC is vital in mitigating risks associated with all military operations.

c. Critical to the evaluation of OPSEC efforts is the review and potential employment of lessons learned and best practices from OPSEC actions through information sharing. The Navy Medicine Security Enterprise utilizes the Joint Lessons Learned Information System (JLLIS) to manage and share lessons and best practices that impact our readiness: https://www.jllis.mil.

5. Policy. In addition to references (a) through (g), NAVMED specific OPSEC policy guidance is listed in subparagraphs 5a through 5f.

a. OPSEC is the commander's program, and they are ultimately responsible for the compliance and effectiveness of their OPSEC program. Commanders and leaders at every level must ensure OPSEC is integrated into all operations and planning, and OPSEC training is conducted per reference (a) and this instruction. NAVMED and every subordinate command must practice OPSEC to deny adversaries' access to CI. The OPSEC Program consists of OPSEC planning, training, education, and evaluation with the goal of creating a culture within BSO-18 staff that protect the information our adversaries seek. Commands must create a positive environment for OPSEC and integrate its principles in the overall framework of information assurance.

b. NAVMED must maintain effective OPSEC that ensures coordination between public affairs, all security disciplines, operations, acquisition, intelligence, training, and command authorities and include mechanisms for enforcement, accountability, threat awareness, and the highest level of leadership oversight. OPSEC protects CI to prevent an adversary from determining friendly intentions or capabilities. Programs must endeavor to establish a proper balance between dissemination of information to families and the public, consistent with the requirement to protect CI and maintain essential secrecy.

c. Social media plays an important role in ensuring a free flow of information to the public; however, it also poses a significant OPSEC risk. To counter the risks inherent with online footprints, all personnel should use the privacy settings of social media web sites to minimize risk and control outside access to one's social media presence. Additionally, considering NAVMED critical information and indicators list (CIIL) listed in enclosure (1), personnel will refrain from posting sensitive command and operations CI on personal or community social media web sites. For a details on writing for public release, refer to your command public affairs office.

(1) Practicing good OPSEC is a family affair, not only at work but at home as well. Be careful not to post movements, deployment dates, ship dates, or when your family members are gone or coming home. If you would not share it with a stranger in person, do not disclose it to strangers online. Even if your page is "private" there are ways for bad actors to acquire information.

(2) Do not disclose or publicly disseminate or reference information as identified by the commands' CIIL and sensitive information already compromised. This provides further unnecessary exposure of the compromised information and may serve as validation. Carefully review other information prior to posting. Seek advice from the appropriate OPSEC coordinator or public affairs office prior to posting questionable content, including photographs and other imagery. Do not post information relating to plans, policies, programs, or operations unless approved for public release by an authoritative source.

d. Commanders, commanding officers (CO), and officers in charge (OIC) must take all OPSEC measures required to prevent disclosure of CI and maintain essential secrecy.

e. OPSEC reporting and mitigation of CI disclosure. All personnel are required to report, as soon as discovered, any inadvertent disclosure or finding of CI not being transmitted, disseminated, protected, or destroyed according to this instruction, or any violation of OPSEC polices to their command OPSEC team. OPSEC violations should, at minimum, be documented and reported to the commanding officer, and to higher headquarters, and a refresher OPSEC course should be directed.

f. OPSEC information must be transmitted in a manner that reduces the risk of aggregation and compromise. Where practicable, a classified network (either data or phone) is the preferred method of transmission for CI. When a classified network is not available, and the information is solely controlled unclassified information (CUI), then it may be transmitted over an unclassified network so long as it is encrypted. Unencrypted transmission of CI over an unclassified network is not authorized.

g. All OPSEC CI, which is categorized as CUI, must be destroyed so it cannot easily be reconstructed and is deemed unrecognizable per reference (b). Classified material must be destroyed per reference (c). OPSEC information may be contained within, but are not limited to: working papers, budgets, briefings, meeting notes, printed e-mails, handwritten memorandums, and manuals or operating instructions.

(1) As a best practice, it is recommended that each activity designate, at a minimum, 1-day per calendar year as a "clean out" day to reduce the amount of the classified and CUI on hand, subject to retention requirements, and destroy the material per references (b) and (c).

(2) If common area recycle bins are used, these bins must be locked with a small slot for paper insertion at the top of the bin to protect the material from inadvertent disclosure or

discovery. When this bin is emptied and the contents are scheduled for shredding, a representative from the command OPSEC team will provide oversight on this process to ensure the contents are being properly destroyed, which includes monitoring the transporting of the bins to the shredding vehicle.

(3) Per references (b) and (c), the method of destroying classified and CUI material within BSO-18 is use of crosscut shredders listed on the National Security Agency Evaluated Products List available at https://www.nsa.gov/Resources/Media-Destruction-Guidance/NSA-Evaluated-Products-Lists-EPLs.

6. Countermeasures. To prevent inadvertent disclosure of unclassified sensitive information and specific CI-related items, all personnel will ensure, at a minimum:

a. Personal actions do not divulge sensitive information inappropriately. Avoid discussing exercises or operations on airlines, in restaurants, during telehealth discussions, or in other public places in addition to phone, texting, e-mail, or chat.

b. When ready for disposal, all paper either printed or handwritten (including but not limited to reports, briefings, meeting notes, user manuals, or operating instructions), regardless of classification, must be destroyed so it is unrecognizable and not discarded in trash cans or recycle bins. This applies to items generated by command personnel and those received from outside sources. This instruction does not apply to classified material; all classified material should be handled and destroyed, per reference (c).

c. Insist on the use of secure terminal equipment phones in secure mode, secure voice-over-internet-protocol, and secure video equipment to communicate CI. Do not attempt to "talk around" sensitive or classified information.

7. BSO-18 Considerations for the Internet

a. Proper OPSEC training is paramount for responsible use of internet-based capabilities like texting, social media, user generated content, social software, e-mail, instant messaging, and discussion forums. To avoid any disclosure of CI, all personnel should be cognizant of the risks of improper disclosure of information via internet-based capabilities. It is incumbent upon all personnel to maintain proper knowledge of the command CIIL and risks associated from using internet-based capabilities such as a possible increased vulnerability to protected personal information.

b. Navy Medicine encourages personnel to responsibly engage in unofficial internet postings about the Department of the Navy (DON) and DON-related activity. If there are any concerns regarding these postings refer to your local public affairs office for guidance.

8. OPSEC Program Management Responsibilities

a. Commanders are ultimately responsible for the compliance and effectiveness of their OPSEC program. Management of the program can be delegated to a program manager designated in writing, whom has unimpeded access to the commanding officer, per reference (e).

b. All personnel assigned or attached to BSO-18 must read and understand this instruction and exercise OPSEC in the daily execution of their assigned duties and be familiar with their local command's OPSEC policy.

c. Specific Responsibilities. In addition to the responsibilities outlined above, the listed specific responsibilities apply:

(1) Chief, BUMED (BUMED-N00):

(a) Designate Director, Mission Assurance (BUMED-N45) overall responsibility for the BSO-18 OPSEC Program. This OPSEC program manager must be a U.S. citizen, in the grade of O-3 or General Schedule-13 or above, have visibility into major NAVMED operations, and must possess and maintain, at a minimum, a favorably adjudicated Tier 3 background investigation with SECRET access.

(b) Utilize JLLIS to collect, validate and disseminate OPSEC lessons learned and best practices.

(2) Directors Maritime Headquarters (BUMED-N03) and Director, Maritime Operations Center (BUMED-N04):

(a) Designate, in writing, an OPSEC Coordinator from each BUMED N-code to serve as the BSO-18 subject matter expert at the NAVMED OPSEC working group. They may only be military or civilian, E-6 or above and GS-9 or higher, per references (e) and (f).

(b) Ensure they receive the training listed in enclosure (2) of this instruction.

(3) NAVMED OPSEC Program Manager:

(a) Responsible for developing and maintaining this instruction and administering the OPSEC Program, per references (a) though (g).

(b) Advise the Chief, BUMED, or their representative, on OPSEC vulnerabilities and requirements.

(c) Coordinate OPSEC requirements and act as the NAVMED representative on all matters pertaining to OPSEC for the enterprise.

(d) Establish and chair the NAVMED OPSEC working group, meeting at least quarterly. Maintain and update the BUMED CIIL via the working group.

(e) Maintain oversight of the regional OPSEC program managers including BUMED Headquarters and conduct an annual assessment of their OPSEC program.

(f) Develop and maintain an OPSEC checklist to be used during assessments to include Medical Inspector General inspections.

(g) Attend the Navy OPSEC program manager course, or any relevant interagency course, within 90 days of designation.

(h) Ensure OPSEC education and training is conducted per this instruction and references (a) through (g).

(i) Ensure JLLIS is used for OPSEC information sharing of best practices.

d. Director, Education and Training (BUMED-N7). Will ensure that annual OPSEC training is included on the BSO-18 annual training plan.

e. Medical Inspector General (BUMED-N00IG). Will incorporate OPSEC inspection line items into the existing OPSEC checklist for inspection of this program. This checklist is maintained on the BUMED Medical Inspector General SharePoint site.

f. Commanders, Naval Medical Forces Atlantic, Naval Medical Forces Pacific, and Naval Medical Forces Development Command:

(1) Designate an echelon 3 Regional OPSEC program manager, in writing, that meets the criteria in reference (e), and provide the signed designation letter to the NAVMED OPSEC program manager. They must not be a public affairs officer or member of the public affairs staff to prevent any possible conflict of interest per reference (e). If a waiver is needed, see enclosure (3).

(2) Develop a regional OPSEC instruction. Refer to reference (e) for the requirements.

(3) Establish and chair a regional OPSEC working group with subject matter experts from all departments, refer to enclosure (4) of this instruction.

g. Commanders, COs, and OICs of Echelon 4 and Echelon 5 Commands:

(1) Exercise overall responsibility for their respective command OPSEC policy, oversight; resourcing, training, reporting, and implementation of responsibilities, per references (a) through (g).

(2) Designate an OPSEC program manager in writing that meets the criteria in reference (e) and provide the signed letter to the immediate superior in charge OPSEC program manager. They must not be a public affairs officer or member of the public affairs staff to prevent any possible conflict of interest, per reference (e).

(3) Ensure the OPSEC program manager attends the Navy OPSEC Program Manager course or any relevant interagency courses within 90 days of being designated to include completion of the additional training listed in enclosure (2) of this instruction.

(4) Provide OPSEC oversight to all subordinate commands and detachments to ensure compliance with all OPSEC guidance.

(5) Conduct a biannual OPSEC program assessment of subordinate commands using the assessment checklist created by BUMED-N45. This checklist is a living document and disseminated to all commands as it is updated. The NAVMED checklist incorporates the checklists listed in references (d), (e), and (g). Upon completion of the signed final assessment report, submit a copy to the immediate superior in charge OPSEC program manager within 15 days of signature.

(6) Develop a local OPSEC instruction. Refer to reference (e) for the requirements.

(7) Develop a localized CIIL and ensure the widest dissemination. Research and development activities should consult the program protection plan during CIIL development.

h. <u>OPSEC Program Managers at All Levels</u>:

(1) Advise Commanders, CO, or OICs on OPSEC matters.

(2) Conduct an annual self-assessment and keep on file for 2 years.

(3) Integrate OPSEC into the commands day-to-day activities to the fullest extent (screensavers, plan of the day, all hands, etc.) to include all plans, operations, exercises and awareness campaigns as appropriate.

(4) Ensure localized OPSEC training is conducted during onboarding or prior to approving personnel for initial network access, as well as an annual refresher administered to all NAVMED personnel.

(a) The initial orientation is intended to provide employees a degree of understanding of general and local OPSEC policies and doctrine commensurate with their responsibilities, per references (e), (f), and (d).

(b) Training should be supplemented with social media awareness and vulnerabilities; local threats; how to protect, transmit and destroy controlled unclassified information; and the requirement for an OPSEC review of information prior to public release.

(5) Maintain a turnover binder, which can be electronic, to ensure OPSEC programs and plans are exercised or evaluated through regular assessments.

(6) At least quarterly, review and provide guidance on BSO-18 and command sponsored web sites and other forms of social media susceptible to inadvertent CI disclosure.

(7) Assist the local public affairs office in conducting a review of documents prior to public release. This multilayer review should include but is not limited to: a review of the document against the commands CIIL, determine if the information is already publicly available, widely known, useful to adversaries or otherwise sensitive.

(8) Coordinate family outreach with the command's ombudsman, if applicable.

(9) Ensure the commanders, COs and OICs OPSEC guidance (e.g., CIIL, memorandums, standard operating procedures, OPSEC Implementation Plans) is widely disseminated.

(10) Assist in developing and recommending guidance and implementing countermeasures to mitigate the risk of potential adversary exploitation of critical information and indicators.

(11) Establish and chair the local OPSEC working group, refer to enclosure (4) of this instruction.

(12) Ensure all staff listed in enclosure (2) of this instruction receive the training annotated, track initial completion and refresher as needed, per this instruction and reference (e).

(13) Although recommended for all commands, operational commands that conduct sensitive missions, operations, or testing and evaluation must additionally develop an OPSEC plan per the template of enclosure (6) of reference (e) to manage signatures that reveal CI.

(14) Coordinate with other OPSEC program managers located in the same facility and or base to implement OPSEC awareness, training, and assessments.

(15) Regularly review and provide guidance on BSO-18 sponsored web sites and other forms of BSO-18 media for inadvertent CI disclosure

i. Contracting Officers Representative:

(1) Complete OPSEC training listed in enclosure (2) within 90 days of appointment to position. Forward certificates of completion to the local OPSEC program manager to keep on file for duration of assignment or designation.

(2) Beginning with the solicitation phase, ensure the local OPSEC program manager is part of the contract process to ensure classified and unclassified contract requirements properly reflect OPSEC responsibilities when applicable per references (d) and (g) and enclosure (5) of this instruction. OPSEC requirements levied on contractors may include but are not limited to:

(a) OPSEC measures the contractor is required to follow.

(b) OPSEC awareness training.

(c) Participation in the command or unit OPSEC program.

(3) Enforce contract requirements related to OPSEC.

9. Records Management

a. Records created as a result of this instruction, regardless of format or media, must be maintained and dispositioned per the records disposition schedules located on the DON Directorate for Administration, Logistics, and Operations, Directives and Records Management Division portal page at https://portal.secnav.navy.mil/orgs/DUSNM/DONAA/DRM/Records-and-Information-Management/Approved%20Record%20Schedules/Forms/AllItems.aspx.

b. For questions concerning the management of records related to this instruction or the records disposition schedules, please contact the local records manager or the DON Directorate for Administration, Logistics, and Operations, Directives and Records Management Division program office.

10. Review and Effective Date. Per OPNAVINST 5215.17A, Director, Logistics, Supply, and Support (BUMED-N4) will review this instruction annually around the anniversary of its issuance date to ensure applicability, currency, and consistency with Federal, Department of Defense, Secretary of the Navy, and Navy policy and statutory authority using OPNAV 5215/40 Review of Instruction. This instruction will be in effect for 10 years, unless revised or cancelled in the interim, and will be reissued by the 10-year anniversary date if it is still required, unless it

meets one of the exceptions in OPNAVINST 5215.17A, paragraph 9. Otherwise, if the instruction is no longer required, it will be processed for cancellation as soon as the need for cancellation is known following the guidance in OPNAV Manual 5215.1 of May 2016.

D. K. VIA

Releasability and distribution:
This instruction is cleared for public release and is available electronically only via the Navy Medicine Web site, https://www.med.navy.mil/Directives/

NAVY MEDICINE BASELINE
CRITICAL INFORMATION AND INDICATORS LIST

1. The success of our NAVMED mission depends on our personnel performing their duties to the utmost of their abilities. Our success also hinges on maintaining good OPSEC. Providing our adversaries knowledge of our strengths and weaknesses could jeopardize the success of our mission and even cost the lives of our Shipmates.

2. Knowing what CI can be harmful if released to our adversaries is key to practicing good OPSEC. To this end, the development and frequent update of a CIIL is vital. It is the responsibility of all hands to know what information is deemed critical in order to avoid its inadvertent disclosure to our adversaries.

3. When developing a local CIIL, ensure it is tailored to each command and their specific functions, consideration should include those geographically separated detachments and that the list is reviewed at least annually and updated as needed. When identifying CI, consider information pertaining to operational aspects such as critical infrastructures, facilities, and equipment, acquisition of products and services, and Research, Development, Test, and Evaluation efforts, in addition to information related to traditional military operations, functions, and activities.

4. When developing an effective local command CIIL, strive to keep it unclassified to ensure the widest dissemination. Everyone understands that classified information must be kept confidential, but they may not realize unclassified information should also be protected. Keep in mind the characteristics listed, the CIIL should be:

a. Based on an upper-echelon CIIL that already exists, but also contain CI specific to that command.

b. Short, contain no more than 10 or 15 items and only sensitive, unclassified items.

c. Easy to read and use terms that everyone understands.

d. Approved by senior leadership with date it was created and approved.

e. Widely disseminated within the organization, division, or element.

5. The NAVMED baseline CIIL listed below can be used as a reference point for commands to develop their own CIIL. The list is not all-inclusive. OPSEC is a systematic, continuous proven cycle which identifies, controls, and protects sensitive but unclassified information regarding a mission, operation, or activity by denying or mitigating an adversary's ability to compromise or interrupt a mission, operation, or activity.

(1) Administrative Indicators.

(a) Personnel rosters, organizational charts and command staff directories.

(b) Flag officer and general officer's schedules, travel plans and itineraries.

(c) Emergency or continuity of operations plans for NAVMED facilities or activities.

(d) Training deficiencies impairing mission accomplishment.

(2) Operations Indicators.

(a) Troop movement, operation plans, force structure and allocation, rules of engagement.

(b) Location (i.e., locations of expeditionary medical facilities in support of operation plans), unit size, equipment, specifications, limitations, and shortfalls.

(c) Capabilities, gaps, and shortfalls (i.e., gaps of naval expeditionary health service support to the fleet or United States Marine Corps).

(d) Training and deployment locations that would reveal military and personnel assignment locations.

(e) Locations of pre-positioned expeditionary medical facilities or activities.

(3) Communications and Infrastructure. Network and technical system architectures, vulnerability information, security assessment reports or physical security weaknesses.

(4) Antiterrorism and force protection information and reports to include force protection condition specific and random antiterrorism measures.

(5) Emergency management plans (not emergency management policy) to include pandemic or public health emergency response plans.

(6) Continuity of Operations (COOP) procedures, dates, locations, and purpose of COOP exercises or scenarios, procedures for conducting vulnerability assessments.

(7) New equipment capabilities and or limitations or changes or shortages in equipment, supplies and or command status that may impair mission capabilities.

OPERATIONS SECURITY TRAINING

TRAINING COURSE	OPSEC PROGRAM MANAGER	OPSEC COORDINATOR	OPSEC WORKING GROUP MEMBERS	CONTRACTING	PUBLIC AFFAIRS	WEB SITE ADMIN	INSPECTION TEAM (OPSEC Rep)	TRAINING LOCATION
Navy OPSEC Course (or OPSE-2380 & OPSE-2390)	X	X	O	O	O	O	O	Navy OPSEC Support Team
OPSE-1500	X	X	X	X	X	X	O	National Counterintelligence and Security Center
CLC-107, OPSEC Contract Requirements	X	X*	X*	X	O	O	O	Defense Acquisition University
Introduction to Information Security- IF011.16	X	X	X	O	X	O	O	Center for Development of Security Excellence
X = Required X* = Required if Review contracts O = Optional	Web sites: - Navy OPSEC Support Team - https://www.navifor.usff.navy.mil/opsec/ - National Counterintelligence and Security Center - https://www.dni.gov/index.php/ncsc-what-we-do/operations-security • OPSE-2380 & OPSE-2390 can be located on this site. - Defense Acquisition University - https://www.dau.edu/ - Center for Development of Security Excellence - https://www.cdse.edu/							

8 Jul 2024

SAMPLE OPERATIONS SECURITY PROGRAM MANAGER WAIVER
(command letterhead)

DD Mmm YY

From: Commanding Officer, [Activity Name]
To: Director, Mission Assurance, Bureau of Medicine and Surgery (BUMED-45)
Via: [Immediate Superior in Charge]

Subj: WAIVER REQUEST FOR COMMAND OPERATIONS SECURITY PROGRAM MANAGER

Ref: (a) SECNAVINST 3070.2A
(b) CNO WASHINGTON DC 131700Z Dec 16 (ALNAV 072/16)

1. Per reference (a) the operations security program manager is required to be a lieutenant (O-3) or above or civilian General Service-12 or higher. Reference (b) automatically grants a waiver of this requirement if program managers are warfare qualified information warfare officers chief warrant officer 2 or above at commands below the echelon 2 level.

2. This paragraph is your reason for requesting the waiver, provided the commands' OPSEC program manager meets all other requirements of reference (a). Due to the small size of the command, [activity title], does not have the manpower to support this requirement, nonoperational mission, etc.]

3. Respectfully request the requirements set forth in the references (a) and (b) be waived. [activity title] OPSEC program manager will be [Ms.; Chief Petty Officer; or Lieutenant (Junior Grade) John Q. Public at john.q.public.civ@health.mil or (619) 555-1234].

commanding officer

8 Jul 2024

OPERATIONS SECURITY WORKING GROUP

1. Each command must convene an OPSEC working group at least quarterly to assist the OPSEC program managers in applying the five-step OPSEC cycle to the command per references (e) and (g). At a minimum, the OPSEC working group will review and update the local CIIL, understand the evolving threat to CI, assess the vulnerability and risk, and implement effective OPSEC measures and countermeasures with the involvement of all elements of the command.

2. An OPSEC working group must include representatives of all key command components, departments, or functions, it must include, at a minimum, representatives from:

a. OPSEC coordinator from all N-codes.

b. Activity security manager.

c. Public affairs office, Web administrators, and social media managers.

d. Antiterrorism and force protection.

e. Insider threat.

f. Cybersecurity.

g. Contracting.

h. Ombudsman.

i. BUMED Secure Internet Protocol Router Program Manager (ad hoc).

j. Privacy Coordinator.

k. BUMED echelon II privacy officer (ad hoc).

l. Others as required or invited.

3. Minutes must be kept of OPSEC working group meetings, distributed within 10-working days of meeting and retained for review.

8 Jul 2024

OPERATIONS SECURITY IN CONTRACTS

1. It is essential to integrate OPSEC into the earliest stages of the acquisition, beginning with generating operational capabilities requirements and continuing through the award, design, development, test and evaluation, fielding, sustainment, and completion process. OPSEC requirements within acquisition and contracting must ensure CI and indicators are not prematurely released to vendors and the public. This applies to all types of contracts, including, but not limited to, service, support, acquisition, and fundamental research and grants.

2. OPSEC program managers or contracting specialists who attended a certified OPSEC officer course, in coordination with the contract requirement owners of the command, are responsible for reviewing contract documents to ensure CI and indicators are withheld from the public. Use an approved CIIL as a reference when conducting reviews.

3. If a contract document contains CI and indicators associated with the performance of the contract, the requesting command develops an OPSEC plan to protect that information associated with the contract throughout the lifecycle of the contract. Refer to reference (e) for an OPSEC plan template.

4. All contractor personnel are required to receive sufficient training to maintain essential secrecy and at least meet the training requirements listed this instruction and in reference (e).

5. Contracts are required to list OPSEC requirements or clauses. If the command has National Industrial Security Program contracts (or classified contracts), a DD 254, Contract Security Classification Specification, is required, and the OPSEC clauses will be listed on the form as well as the contract. A DD 254 is not required for Non-National Industrial Security Program contracts (or unclassified contracts) therefore the OPSEC clauses will be listed within the contract itself.

6. For more detailed information on OPSEC as it relates to acquisitions and contracts including examples of contract language refer to appendix G of reference (g).