



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

IN REPLY REFER TO  
BUMEDINST 3070.1  
BUMED-M4  
19 Dec 2015

BUMED INSTRUCTION 3070.1

From: Chief, Bureau of Medicine and Surgery

Subj: OPERATIONS SECURITY

Ref: (a) CJCSI 3213.01D  
(b) DoD Directive 5205.02E of 20 June 2012  
(c) JP 3-13.3, Operations Security  
(d) NTTP 3-54M/MCWP 3-40.9 (NOTAL)  
(e) DoD 5205.02-M, DoD Operations Security (OPSEC) Program Manual of  
3 November 2008  
(f) OPNAVINST 3432.1A  
(g) SECNAVINST 5510.30B  
(h) DON CIO WASHINGTON DC 032009Z Oct 08  
(i) SECNAV M-5510.36  
(j) SECNAVINST 5211.5E

Encl: (1) Operation Security Process  
(2) Budget Submitting Office 18 100 Percent Paper Destruction Policy  
(3) Bureau of Medicine and Surgery E-mail Digital Signature and Encryption Policy  
(4) Acronym List

1. Purpose. To implement policy prescribed in references (a) through (j), and enclosures (1) through (4), assign responsibilities for the Bureau of Medicine and Surgery's (BUMED) Operations Security (OPSEC) Program, and direct planning actions to identify and protect classified and unclassified, yet critical, mission information and operations.

2. Scope and Applicability. The provisions of this instruction are applicable to all military, civilian, and Government contractor personnel in all echelons of Navy Medicine and Budget Submitting Office (BSO) 18 activities.

3. Background

a. OPSEC is critical to the success of U.S. Navy activities. Maintaining OPSEC of plans and movements maximizes the element of surprise and is essential to maintaining freedom of action. OPSEC attempts to prevent the inadvertent compromise of unclassified or sensitive activities, capabilities, or intentions at every level of war. The purpose of OPSEC is to reduce the vulnerability of friendly forces from successful adversary exploitation of critical information (CI).

b. OPSEC is a core competency within information operations. For commands planning at the strategic and operational levels, OPSEC processes provide an integrated conduit for

protecting CI while disrupting, denying, and degrading the adversary's attempts to gain an advantage. For commands at the tactical level executing plans and carrying out operations, proper utilization of OPSEC planning, tracking, and execution provides an increased probability of success by preventing the timely aggregation and analysis of CI required for the adversary to disrupt friendly actions.

c. Reference (a) identifies OPSEC as one of three key components for achieving operational success. The other two components are security programs and counterintelligence. The important distinction between OPSEC and the other components is that OPSEC is an operational function rather than a security function. Additionally, OPSEC focuses on unclassified activities, information and vulnerabilities, whereas security functions (physical security, information security systems, etc.) are primarily directed towards the protection of classified material. As an operational function, OPSEC belongs in daily activity planning and must continually be revisited as the command's mission and vision transform.

d. The OPSEC process recognizes that risk is inherent to all military activities. Proper use of the OPSEC process will achieve a balance, maximizing information security, while minimizing the impact on operations and planning requirements. The command and OPSEC planning must evaluate each operation to determine the most effective countermeasure(s) for implementation, balanced against operational requirements, timelines, and budget.

e. CI is information about Department of Defense (DoD) activities, intentions, capabilities, or limitations that an adversary seeks in order to gain a military, political, diplomatic, economic, or technological advantage. Such information, if revealed to an adversary, may prevent or degrade mission accomplishment, cause loss of life, or damage friendly resources. If obtained, CI will either impact the success of BSO-18 or improve the likelihood of an adversary meeting their goals.

f. To protect CI, all personnel must abide to OPSEC policy and develop countermeasures that mitigate the risks of divulging CI. OPSEC measures are required for:

(1) Operations and activities related to the preparation, deployment, and sustainment of the U.S. Navy in times of war, crisis, or peace. OPSEC applies to all activities that prepare, sustain, or employ forces.

(2) The protection of information contained in operations plans, supporting plans, and orders.

4. Policy. In addition to references (a) through (j), the following is BUMED specific OPSEC policy guidance.

a. BUMED OPSEC Vision. OPSEC is the commander's program. Commanders and leaders at every level must personally ensure OPSEC is integrated into all operations and

planning, and OPSEC training is conducted per this instruction. Enclosure (1) provides additional guidance on the OPSEC process. BUMED 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 ultimate goal of creating a culture of BSO-18 staff that protect the information our adversaries seek. Although OPSEC is not intended to be a security discipline, and will not replace program security requirements, OPSEC does significantly contribute to the overall security posture of the command. Commands must create a positive environment for OPSEC and integrate its principles in the overall framework of information assurance.

b. OPSEC Program. The OPSEC Program is the means by which BUMED and its components protect unclassified CI. Every OPSEC Program is developed at the command level, and carried out by OPSEC program managers, OPSEC officers, and OPSEC coordinators. The OPSEC Program specifies the training plan, objectives, schedule, and standards for OPSEC training. The program reflects the commander's intent, makes OPSEC a priority, integrates OPSEC into training and awareness programs, force protection and operational planning, and continually assesses an organization's ability to apply appropriate OPSEC practice in its daily mission. References (a) through (f) mandate the existence of a BUMED OPSEC Program.

5. Objectives. The OPSEC Program's overall objective is to enhance the security posture of BUMED and Navy Medicine, specifically:

- a. Train and familiarize personnel at all organizational levels in the application of OPSEC.
- b. Plan and execute OPSEC actions in military operations and exercises.
- c. Deny adversary decision maker access to CI.

6. Organization. All BUMED and Navy Medicine commands must have an OPSEC program manager appointed in writing per reference (e).

a. OPSEC Program Manager (BUMED-M45). BUMED-M45 is the OPSEC program manager. The OPSEC program manager is the primary staff member responsible for the integration of OPSEC into all BUMED/Navy Medicine commands, and ensures the implementation of OPSEC in all operations and has oversight of all subordinate OPSEC programs per reference (e). The OPSEC program manager is responsible for maintaining this instruction, chairing the OPSEC working group, and completing the duties outlined in references (a) through (f). The OPSEC program manager must be in the grade of O-4 or GS-13 or above, must have visibility into major BUMED/Navy Medicine operations, and must possess a TOP SECRET clearance. The following is a list of duties to be performed by the BUMED OPSEC program manager:

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

(2) Recommend OPSEC guidance and mitigations.

(3) Maintain and update the BUMED CI list, approved by the Chief, BUMED.

(4) Coordinate Navy Medicine OPSEC requirements.

(5) Chair the OPSEC working group and ensure it meets at least quarterly to review OPSEC requirements and assess operations per references (a) through (f).

(6) Supervise the OPSEC officers from BUMED, Navy Medicine, and subordinate commands, and ensure they complete annual assessments and triennial surveys. Provide support and guidance to other OPSEC managers and coordinators for whom the OPSEC program manager has oversight.

(7) Coordinate policy and requirements with security program managers.

(8) Coordinate with the Office of the Secretary of the Navy for OPSEC policy recommendations.

(9) When necessary, participate in the review process of information for public release.

(10) Ensure, at a minimum, initial and annual OPSEC refresher trainings are administered to 100 percent of BUMED and subordinate command's military, civilian, and government contractor personnel.

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

b. OPSEC Working Group. The BUMED OPSEC program manager, assisted by the regional OPSEC program managers, must lead the OPSEC working group and the annual OPSEC assessment. At a minimum, the OPSEC working group will review and update BUMED CI, conduct analysis of OPSEC threats, vulnerabilities, assess the risks, make recommendations for implementing OPSEC measures, and conduct OPSEC training for the staff. The OPSEC working group, at a minimum, will consist of representatives from the following codes:

(1) BUMED OPSEC Program Manager.

(2) Navy Medicine Regional OPSEC Program Managers.

(3) BUMED Information Systems Security manager.

(4) BUMED Antiterrorism/Force Protection officer.

(5) Naval Criminal Investigation Service representative, if available and may be an adhoc member.

(6) Public Affairs officer (BUMED-M09B7).

7. Responsibilities. OPSEC is a command responsibility. Specific responsibilities are:

a. Chief, BUMED must:

(1) Have overall responsibility for formulation and dissemination of BSO-18 OPSEC program per references (a) through (e);

(2) Designate a BSO-18 OPSEC program manager in writing and provide sufficient resources, staff assistance, and authority to implement, manage, and execute an effective OPSEC Program;

(3) Provide OPSEC guidance to subordinate commands;

(4) Identify OPSEC measures and coordinate execution with other commands, as necessary;

(5) Conduct OPSEC surveys and annual assessments as required;

(6) Conduct annual OPSEC Program reviews;

(7) Conduct OPSEC training at command indoctrinations annually, at a minimum, for all military, civilian, and government contractor personnel;

(8) Promote an understanding and awareness campaign among BSO-18 personnel of the OPSEC process, command CI, adversary intelligence threats (in concert with the Naval Criminal Investigative Service and command security manager) wireless communication vulnerabilities, and individual OPSEC responsibilities; and

(9) Ensure the exercise of OPSEC oversight for contracts per references (a) through (f).

b. Commanders, Navy Medicine East; Navy Medicine West; and Navy Medicine Education and Training Command must:

(1) Establish a command OPSEC Program that incorporates formal schools, training, planning, and evaluation tailored to the missions and functions of the command per references (a) through (g);

(2) Designate an OPSEC program manager in writing and provide the name and contact data to the BUMED OPSEC program manager. The OPSEC program manager must assist commanding officers (CO) and officers in charge (OIC) in identifying CI per references (c) and (d);

(3) Provide OPSEC oversight to all subordinate commands to ensure compliance with all OPSEC guidance;

(4) Identify command CI for appropriate commands and public affairs offices;

(5) Conduct yearly OPSEC assessment per references (a) through (f);

(6) Ensure command OPSEC program manager attends the Navy or DoD OPSEC Program Manager's course;

(7) Ensure that OPSEC is integrated into all plans, operations, and exercises as appropriate;

(8) Ensure counterintelligence training is conducted annually per reference (g);

(9) Conduct OPSEC training at command indoctrination annually, at a minimum, for all military, civilian, and Government contractor personnel;

(10) Per enclosure (2), implement 100 percent destruction policy for all paper products with printed or handwritten data; and

(11) Coordinate OPSEC measures and execution with other commands as necessary.

c. COs and OICs of Navy medical centers and naval hospitals, tenant medical treatment facilities, and all other activities must:

(1) Establish a command OPSEC Program that incorporates formal schools, training, planning, and evaluation tailored to the missions and functions of the command per references (a) through (g);

(2) Designate an OPSEC program manager in writing and must provide the name and contact data to the BUMED OPSEC program manager. The OPSEC program manager must assist COs and OICs in identifying CI per references (c) and (d);

- (3) Provide OPSEC oversight to all subordinate commands to ensure compliance with all OPSEC guidance;
- (4) Identify command CI for appropriate commands and Public Affairs offices;
- (5) Conduct yearly OPSEC assessment per references (a) through (f);
- (6) Ensure command OPSEC program manager attends the Navy or OPSEC Program Managers Course;
- (7) Ensure that OPSEC is integrated into all plans, operations, and exercises, as appropriate;
- (8) Ensure counterintelligence training is conducted annually per reference (g);
- (9) Conduct OPSEC training at command indoctrination annually, at a minimum, for all military, civilian, and Government contractor personnel;
- (10) Implement a 100 percent destruction policy for all paper products with printed or handwritten data; and
- (11) Coordinate OPSEC measures and execution with other commands as necessary.

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

- a. Ensure that personal actions do not divulge sensitive information inappropriately. Avoid discussing exercises or operations on airlines, in restaurants, or in other public places in addition to phone, texting, e-mail, or chat.
- b. Report suspected Foreign Intelligence Service (FIS) encounters to the command security manager. FIS operatives may attempt to collect information via social engineering techniques such as e-mail phishing, telephone, personal inquiries under the pretext of innocuous legitimate business, or unduly persistent and invasive questions in social situations.
- c. Per enclosure (2), 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 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 (i).
- d. When applicable, ensure classified and unclassified contract requirements properly reflect OPSEC responsibilities.

e. Encrypt Nonsecure Internet Protocol Router Network e-mails containing sensitive but unclassified information or items from the CI list per enclosure (3).

f. 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.

g. Critically question the placement of unclassified information on public or even protected networks. Determine if the information really needs to be there, balanced against the risk to inform surrounding personnel to discontinue discussions of sensitive but unclassified information or CI list items until the phone call has ended. OPSEC is more than just putting the right information on a given network, it is also a critical examination of what content needs to be there for mission success.

#### 9. 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 staff CI, all personnel should be cognizant of the risks of improper disclosure of information via internet-based capabilities. It is incumbent upon all divisions to ensure all hands maintain proper knowledge of the BUMED CI list. In addition, all staff personnel must maintain awareness of the risks associated from using internet-based capabilities such as a possible increased vulnerability to protected personal information.

b. BUMED encourages personnel to responsibly engage in unofficial internet postings about the Department of the Navy (DON) and DON-related activity. The Navy and Marine Corps perform a valuable service around the world every day and DON personnel are frequently in a position to share our successes with a global audience via the internet. DON personnel are responsible for all DON-related content they publish and should ensure this content is accurate, appropriate, and does not compromise mission security or success. The following are examples of items Sailors and other staff members may share in a social media forum.

(1) Successful theater security engagements after they happen.

(2) Events depicting credit upon the Navy that will benefit recruitment and retention.

(3) Informative statements per Public Affairs (BUMED-M09B7) guidance.

c. As with other forms of communication, DON personnel are responsible for adhering to DON regulations and policies when making unofficial posts. DON personnel should comply with regulations and policies such as personal standards of conduct, operations security, information assurance, personally identifiable information (PII), joint ethics regulations,

protected health information (PHI) and the release of information to the public. BUMED prohibits all personnel from disclosing any item on the staff CI list. In addition, BUMED discourages personnel from posting the following items:

- (1) Culturally insensitive comments
- (2) Disparaging remarks
- (3) False statements
- (4) Statements of a technical nature in or outside the member's expertise
- (5) Protected personal and health information

d. All personnel should be aware that the internet is often used to gain information for criminal activities such as identity theft. By piecing together information provided on different Web sites, criminals can use the information to, among other things, impersonate DON personnel, steal passwords, and compromise DON networks. When using the internet and social media, all personnel should be cautious and guard against cyber criminals and attackers by adhering to the proper security procedures.

e. All official information which is being released or posted on internet Web sites must be reviewed by the command, regional or BUMED OPSEC program manager.

10. OPSEC Self-Reporting. BUMED encourages all personnel to self-report OPSEC violations to the BUMED OPSEC program manager, regional OPSEC program manager, or the local commands' OPSEC program managers in order to mitigate possible consequences.

11. Summary. To prevent adversaries from gaining actionable intelligence about friendly operations, BUMED and subordinate commands must be vigilant in planning and executing OPSEC measures. To be most effective, OPSEC measures must be considered as early as possible during mission planning and then be appropriately revised to keep pace with changes in current operations and threats.

12. Records. Records created as a result of this instruction, regardless of media and format, shall be managed per SECNAV M-5210.1 of January 2012.

  
C. FORREST FAISON III

Distribution is electronic only via the Navy Medicine Web site at:  
<http://www.med.navy.mil/directives/Pages/BUMEDInstructions.aspx>

## OPERATION SECURITY PROCESS

1. General. OPSEC planning is accomplished through the use of the OPSEC process. This process provides the information required to write the OPSEC section of any plan or order. OPSEC planning is done in close coordination with the overall planning effort and with the planning of the OPSEC working group.
2. Strategy. OPSEC involves the application of a systematic analytical process to determine how adversaries derive CI of value to them. The OPSEC process identifies the CI or “core secrets” of an operation that must be kept from an adversary if the operation is to succeed, and applies necessary countermeasures to deny that information to the adversary. OPSEC deals with information that, when collected in pieces and combined in aggregated form, could reveal sensitive classified aspects of an operation. View your operation from the adversary’s perspective.
3. Five Phases to the OPSEC process. These phases do not have to be done in order. You may go from one to the other as you develop OPSEC awareness for your area.
  - a. Phase One - Identification of CI. You need to ask yourself, “What am I doing that I would not want an adversary to know?” “What am I doing that would be of value to my adversaries?” “Who are the adversaries and what tactics might they use to act against us?” “What information would they need to support these tactics?” It may be one or more of the following:
    - (1) What do we intend to do?
    - (2) When will we do it?
    - (3) Where will we do it?
    - (4) How many will do it?
    - (5) What technology will we use?
    - (6) What do we know?
    - (7) Do we know about the adversary?
  - b. Phase Two - Analysis of the Threat:
    - (1) Who are your adversaries?
    - (2) Who are the adversaries' allies and will they share CI?

(3) What might the adversaries already know about your operation through open sources, casual observation, or surveillance?

- (a) Specific mission or project
- (b) Specific locations
- (c) Specific adversaries
- (d) Specific collection methods
- (e) Specific threats from adversaries

(4) What are the adversaries' interests?

(5) What are the adversaries' capabilities to do damage or exploit the information, and what are the potential strategies?

(6) What do the adversaries already know?

(7) What must the adversaries know and when?

(8) How might the adversaries get information?

(9) Could the knowledge of your CI permit an adversary to initiate actions that would negate, impair, or degrade the effectiveness of your activity or maneuver within the battlespace?

c. Phase Three - Vulnerability Analysis:

(1) Now that the CI is identified, and the threat characterized, you can analyze your operations from an adversary's viewpoint to determine what their collection strategy could be. This helps to identify where the vulnerabilities are in your operation.

- (a) Do we have patterns which result in predictability?
- (b) What are the indicators of those patterns?
- (c) Should we affect interpretation or deceive (how should we deceive)?

(2) What indicators not already known by the adversary will friendly actions reveal?

(3) What CI can the adversary actually collect?

(4) Can the adversary collect the CI, analyze it, make a decision, and take action in time to interfere with my operations?

(5) Will my OPSEC countermeasures introduce new indicators to the adversary?

d. Phase Four - Risk Assessment:

(1) Taking each vulnerability from phase three, assess the impact to mission if the adversary possessed that information due to compromise.

(2) For those vulnerabilities with unacceptable impact to your operations, the staff must devise countermeasures to minimize or negate the impact. More than one countermeasure may be identified for each vulnerability.

(3) The commander must compare the estimated costs associated with implementing each countermeasure to the potential harmful effects on mission accomplishment resulting from an adversary's exploitation of a particular vulnerability.

(4) Remember, if a countermeasure isn't practical, you probably shouldn't do it.

e. Phase Five - Apply OPSEC Countermeasures:

(1) All countermeasures should possess measures of effectiveness to determine if the countermeasure has the appropriate outcome.

(2) Establish measures of performance to ensure your countermeasures are properly implemented.

(3) Provisions for feedback ensure that a failed countermeasure is communicated back to the staff planning group and successful countermeasures are used again and entered into lessons learned.

BUDGET SUBMITTING OFFICE 18 100 PERCENT  
PAPER DESTRUCTION POLICY

1. Purpose. The purpose of this policy is to implement 100 percent shredding/destruction of generated paper documents that are no longer needed, regardless of classification, to prevent inadvertent disclosure of any classified, controlled unclassified information (CUI), and any specific CI related items. Paper documents include: working papers, budgets, briefings, meeting notes, e-mails, handwritten memorandums, and manuals or operating instructions per reference (j).

2. Situation. This BUMED 100 percent shred policy applies to all DoD, military, civilian, and contractor personnel assigned to BSO-18 commands.

a. When finished with paper documents, destroy ALL paper having either printed or handwritten print on it regardless of classification. This applies to items generated by command personnel and those received from outside sources. Working papers must not be discarded in trash cans or recycle bins.

b. Destroy all classified information that is no longer required for operational purposes. Destruction of classified information must be accomplished by means that eliminate risk of recognition or reconstruction of the information per reference (i).

c. All classification of material pending destruction must be controlled in a manner designed to minimize the possibility of unauthorized removal or access. A burn bag may be used to store any classification of material awaiting destruction. Seal and mark the highest classification of the material inside each burn bag at the highest level of classified material and ensure that all classified and CUI materials are properly contained until actually destroyed.

d. Per reference (j), the method of destroying classified and CUI material within BUMED and BSO-18 is by using National Security Agency (NSA) or the Central Security Service (CSS) approved shredders.

(1) BSO-18 commanders must ensure adequate access to approved shredders, disposal methods for all PII, PHI, or other documents containing sensitive information.

(2) Only shredders listed on the NSA or the CSS evaluated products list for high security crosscut shredders will be used to destroy classified material by shredding.

(3) Only shredders listed on the NSA or CSS evaluated products list for non-critical sensitive material will be used to destroy PII or PHI.

(4) The disposal of computer media (compact discs, digital video devices, hard drives, etc.) containing either classified or unclassified CI must be coordinated through the Director for Information Management and Technology (BUMED-M6B).

3. Unclassified material must be destroyed when there is no longer a requirement for maintaining the material. It is recommended that each directorate designate an annual clean-out day for disposal of unnecessary classified and unclassified material holdings. Continue destruction of classified paper per reference (e).

4. If common area recycling bins are used, these bins must be locked and a small slot for paper insertion will be in the top of the bin. When this bin is emptied and the contents are scheduled for shredding, a representative of the security manager's office will provide oversight on this process to ensure the contents are being properly destroyed.

5. If a commercial shredding company is employed, a chain of custody will be established when taking the recycling bins to the shredding vehicle.

BUREAU OF MEDICINE AND SURGERY E-MAIL DIGITAL SIGNATURE AND  
ENCRYPTION POLICY

1. Purpose. The purpose of this policy is to enforce the Chief Information Officer Policy and Guidance Memorandum for e-mail digital signature and encryption policy per reference (h).

2. Situation. BUMED users must digitally sign e-mail messages requiring either message integrity and/or non-repudiation, and encrypt messages containing CI or PII.

a. Digital Signature

(1) A digital signature is required for all e-mail containing either an attachment (picture, word document, PowerPoint briefing, spreadsheet, etc.) or embedded “clickable” content (“mail to” e-mail links or Web site uniform resource locator addresses).

(2) A digital signature is required for any e-mail that: directs, tasks, or passes direction or tasking; requests or responds to requests for resources; promulgates organization, position, or information external to the organization (division, department, or command); discusses any operational matter; discusses personnel management matters; the need exists to ensure that the e-mail originator is the actual author; or the need exists to ensure that the e-mail was not tampered with in transit.

b. Encryption

(1) All BSO-18 personnel must encrypt e-mail messages containing sensitive, critical, or PII.

(2) PII is defined as: information about an individual that identifies, links, relates, is unique to, or describes that individual. For example: a social security number, age, military rank, civilian grade, marital status, race, salary, home phone number, other demographic, biometric, personnel, medical, and financial information, etc.

(3) PHI is defined as: a record of a patient’s treatment and medical history that includes PII.

ACRONYM LIST

BSO	Budget Submitting Office
BUMED	Bureau of Medicine and Surgery
CI	Critical Information
CO	Commanding Officer
CSS	Central Security Service
CUI	Controlled Unclassified Information
DoD	Department of Defense
DON	Department of the Navy
FIS	Foreign Intelligence Service
NSA	National Security Agency
OIC	Officer In Charge
OPSEC	Operations Security
PHI	Protected Health Information
PII	Personally Identifiable Information