DEPARTMENT OF THE NAVY
U.S. NAVAL SUPPORT ACTIVITY NAPLES ITALY
PSC 817 BOX 1
FPO AE 09622-0001

NAVSUPPACTNAPLESINST 3100.2G
N3
16 Feb 24

NAVSUPPACT NAPLES INSTRUCTION 3100.2G

From: Commanding Officer, U.S. Naval Support Activity, Naples, Italy

Subj: OPERATIONS SECURITY

Ref: (a) DoD Directive 5205.02E of 20 June 2012, DoD Operations Security Program
(b) DoD Manual 5205.02, DoD Operations Security Program Manual of 3 November 2008
(c) NTTP 3-13.3M/MCTP 3-32A, Operations Security
(d) SECNAVINST 3070.2A, Operations Security
(e) OPNAVINST 3432.1A, Operations Security
(f) CNICINST 3070.2, Commander, Navy Installations Command Operations Security Program
(g) DoD Directive 8100.02 of 14 April 2004, Use of Commercial Wireless Devices, Services and Technologies in the Department of Defense Global Information Grid
(h) COMNAVREGEURAFSWAINST 2200.1, Portable Electronic Devices
(i) COMNAVREGEURAFSWAINST 5239.1, External Hard Drive Policy for Unclassified Network
(j) DoN CIO Memorandum of 12 February 2016, Acceptable use of Department of the Navy Information Technology
(k) ALNAV 056/10, 192027Z August 2010, Internet-Based Capabilities Guidance – Official Internet Posts
(l) ALNAV 057/10, 192031Z August 2010, Internet-Based Capabilities Guidance – Unofficial Internet Posts
(m) COMNAVREGEURAFCENTINST 3070.2B, Operations Security Program

Encl: (1) (U) Critical Information List (Contact Operations for info)
(2) Operations Security Considerations for Internet-Based Capabilities
(3) Operations Security Considerations for Public Release of Information

1. Purpose. To establish policy, procedures, and responsibilities for U.S. Naval Support Activity (NAVSUPPACT), Naples, Italy, Operations Security (OPSEC) Program.

2. Cancellation. NAVSUPPACTNAPLESINST 3100.2F

3. Scope and Applicability. All military, civilians, and contractors, to include staff and subordinate commands, conducting operations or services in support of NAVSUPPACT Naples, Italy.

4. General

a. OPSEC is the process of identifying critical and sensitive data, analyzing the threat, determining the vulnerabilities, assessing the risk, and developing and implementing countermeasures. The ultimate goal of OPSEC is increased mission effectiveness. Critical Information (CI) is information that is critically needed by an adversary. Although CI can be classified, the majority is sensitive but UNCLASSIFIED. Though this information can be unclassified, it should still be protected to the highest extent possible.

b. Personnel sharing CI in public, on an unsecured phone line, or with people who do not have a need-to-know should be reported to the OPSEC Program Manager (PM) or Security Manager. Unauthorized sharing of CI can result in administrative or disciplinary action against military and civilian personnel or removal from working on a contract or contracts for contractor employees.

5. Responsibilities. OPSEC is the Commanding Officer's (CO) program. All NAVSUPPACT Naples departments will ensure OPSEC is integrated in all plans and operations. Personnel assigned OPSEC functions must be familiar with and implement references (a) through (m).

a. CO must:

(1) Appoint an OPSEC Program Manager (PM) in writing. The designee must have insight to the full scope of the Command's mission and may manage the OPSEC program full-time or as a collateral duty.

(2) Appoint an OPSEC Officer in writing.

(3) Ensure appointed OPSEC PM and OPSEC Officer have completed all necessary OPSEC training per reference (c).

b. NAVSUPPACT Naples OPSEC PM must:

(1) Establish an OPSEC program that incorporates formal schools, training, planning, and evaluation tailored to Area of Responsibility (AOR), the mission and functions of the command.

(2) Integrate the functions of OPSEC into all concept plans, operation plans, operation orders, and additional planning evolutions.

(3) Implement a 100 percent shred or burn policy for all paper products within the scope of OPSEC.

(4) Coordinate with other OPSEC PMs at tenant commands in order to implement OPSEC awareness, training, and assessments.

c. OPSEC Officer must:

(1) Implement and maintain the OPSEC program for NAVSUPPACT Naples.

(2) Annually assess the level of Command OPSEC awareness and the adequacy of OPSEC training per reference (a).

(3) Coordinate and provide OPSEC support (tools and services) for tenant commands, leveraging Department of Defense OPSEC assets, including Navy Information Operations Command Norfolk, Joint Communications Security (COMSEC) Monitoring Activity, and Joint Information Operations Warfare Command/Joint OPSEC Support Element.

(4) Conduct annual command OPSEC program reviews per references (a), (d), and (e).

(5) Coordinate all OPSEC training for NAVSUPPACT Naples.

(6) Keep the chain of command informed of all OPSEC issues including disclosures, violations, etc. and provide guidance as to the most appropriate course of action.

(7) Maintain an OPSEC turnover binder to ensure continuity of the OPSEC program.

(8) Lead the internal OPSEC Working Group (OWG), as needed.

d. NAVSUPPACT Naples Department Heads or designee must:

(1) Report all OPSEC issues to the NAVSUPPACT Naples OPSEC Officer.

(2) Keep the chain of command informed of all OPSEC issues to including disclosures, violations, etc., and provide guidance as to the most appropriate course of action.

(3) Attend the NAVSUPPACT Naples OPSEC Working Group as required.

e. Public Affairs Officer Webmasters must regularly review and provide guidance on Navy sponsored websites and other forms of media in the NAVSUPPACT Naples AOR for inadvertent disclosures of CI.

f. OWG is a working group which convenes at least quarterly to conduct OPSEC planning and to assess their Command's OPSEC program. The OWG is a cross-functional working group composed of, but not limited to, the following individuals: appointed OPSEC Officer, representatives from the Public Affairs Office, Operations, N6, Security Officer, and the Command Security Manager. The OWG or OPSEC Officer must develop quarterly key talking points for distribution to all NSA Department Heads and Command leadership.

g. All Hands must:

(1) Be familiar with this instruction, including the Critical Information List enclosure (1).

(2) Encrypt all e-mails transmitted via unclassified government computer networks which contain sensitive or CI, including Personally Identifiable Information per reference (g). For additional clarification see enclosure (1).

(3) Shred or burn 100 percent of all items containing critical information.

(4) Adhere to NAVSUPPACT Naples OPSEC considerations for use of social media and internet-based capabilities in enclosure (2).

(5) Complete all training requirements in accordance with this reference.

(6) Report any suspected disclosure of CI to the OPSEC Officer, OPSEC PM, or chain of command.

(7) Understand that failure to follow OPSEC guidance can result in administrative or disciplinary action.

6. Training

a. Military and civilian personnel must receive OPSEC training upon arrival and refresher training each fiscal year at a minimum thereafter. Personnel who are unable to attend OPSEC training will complete Uncle Sam's OPSEC (Course ID number NIOC-USOPSEC-2.0 or newest version available) computer-based training via Navy Knowledge Online.

b. NAVSUPPACT Naples OPSEC training must include, but are not limited to, COMSEC monitoring and prior consent notification, travel and interactions with foreign nationals, as well as information regarding work and personal internet use (i.e., any threats that may be encountered).

c. OPSEC Officers and OPSEC PMs will complete the OPSEC Analysis and Program Management Course (OPSE-2500).

d. Personnel who work with contracts are recommended to complete the OPSEC Analysis and Program Management Course (OPSE-2500) or OPSEC Analysis Course (OPSE-2380).

7. 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 Department of the Navy Assistant for Administration, 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 OPNAV Records Management Program (DNS-16).

8. Review and Effective Date. Per OPNAVINST 5215.17A, NAVSUPPACT Naples will review this instruction annually on the anniversary of its effective 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 automatically expire 10 years after effective date unless reissued or canceled prior to the 10-year anniversary date, or an extension has been granted.

RANDAZZO.JOHN.LUCIAN.1035461376

Digitally signed by RANDAZZO.JOHN.LUCIAN.1035461376
Date: 2024.02.16 14:47:32 +01'00'

J. L. RANDAZZO

Releasability and distribution:
NAVSUPPACTNAPLESINST 5216.4DD
Lists: I through IV
Electronic via NAVSUPPACT Naples website:
https://cnreurafcent.navy.afpims.mil/Installations/NSA-Naples/About/Installation-Guide/Department-Directory/N1-Administration-Department/Instructions

Controlled by: Department of the Navy
Controlled by: NSA Operations
CUI Category(ies): Unclassified
Limited Dissemination Control: FEDCON
POC: LT Adam Tucker, 081-568-0000
adam.m.tucker5.mil@us.navy.mil

OPERATIONS SECURITY CONSIDERATIONS FOR INTERNET-BASED CAPABILITIES

1. Internet-Based Capabilities. Proper Operations Security (OPSEC) training is required for responsible use of internet-based capabilities (SMS texting, social media, user-generated content, social software, e-mail, instant messaging, and discussion forums) to prevent disclosure of critical information. All personnel must be aware of the risks of improper disclosure of information via internet. It is incumbent upon all hands to maintain proper knowledge of the Critical Information List (CIL) and protect personal information. Guidelines and recommendations for using social media in a manner that minimizes risk are located in references (a) and (c). Any additional questions may be addressed to the OPSEC Program Manager, OPSEC Officer, or Public Affairs Officer.

2. Encouraged Social Media Postings. Department of the Navy (DoN) personnel are encouraged to engage responsibly in unofficial internet posting about publicly releasable DoN and DoN related activity. The Navy and Marine Corps perform 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 that this content is accurate, appropriate, and does not compromise mission security or success. The following are examples of information Sailors and other staff members may share in a social media forum.

a. Successful theater security engagements after they are completed.

b. Events reflecting credit upon the United States Navy that are beneficial to recruitment and retention.

c. Informative statements in accordance with public affairs guidance and references (c) through (d).

3. Discouraged Social Media Postings. As with other forms of communication, DoN personnel are responsible for adhering to DoN regulations and policies when making unofficial internet posts. DoN personnel should comply with regulations and policies such as personal standards of conduct, OPSEC, information assurance, personally identifiable information, joint ethics regulations, and the release of information to the public. All personnel are prohibited from disclosing any item on the CIL. In addition, command personnel are discouraged from posting the following items.

a. Culturally insensitive comments.

b. Disparaging remarks.

c. False statements.

d. Statements of a technical nature in or outside the member's expertise.

e. Protected personal information.

4. Website Content. Unclassified, publically available websites must not display personnel lists, "roster boards", organizational charts, or command staff directories which show individual's names, phone numbers, or e-mail addresses which contain the individuals' name. General telephone numbers and non-personalized e-mail addresses for commonly-requested resources, services, and contacts, without individual's names, are acceptable.

5. Security. All staff 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 websites, criminals can use information to impersonate DoN personnel, steal passwords, and compromise DoN networks. Therefore, when using the internet and social media, all personnel should be cautious and guard against cyber criminals and attackers by adhering to proper security procedures.

a. Personal e-mail accounts will not be used for official purposes. CI cannot be sent via commercial e-mail servers (gmail, yahoo, etc.).

b. CI may be sent via an encrypted unclassified e-mail from an official e-mail address when necessary. All personnel are required to publish their e-mail certificates to the Global Address List to ensure they are able to both sign e-mails for verification and send or receive encrypted e-mails.

6. Violations. OPSEC violations are non-punitive/non-attribution and should be self-reported to the OPSEC Officer in order to mitigate possible consequences.

OPERATIONS SECURITY CONSIDERATIONS FOR PUBLIC RELEASE OF INFORMATION

1. Purpose. Establish guidance for Operations Security (OPSEC) review of information intended for public release.

2. Content Review

a. The Public Affairs Office (PAO) is responsible for facilitating open, timely and uninhibited access to public information, except where restricted by law, security classification, or privacy statutes. As such, the authority for public release of information is delegated to the command PAO by the Commanding Officer. The PAO is responsible for establishing a standard procedure for review of information prior to release to the public. This formal process must include an OPSEC review conducted by a properly trained individual.

b. Personnel responsible for reviewing content prior to public release in an official capacity are required to complete OPSEC and Public Release Decisions (OSPE-1500) training. A certificate of completion must be submitted to the Command OPSEC Officer.

c. All information for public release must be reviewed for OPSEC concerns by an OPSEC trained individual prior to release. For Official Use Only, Personally Identifiable Information, and any other information on the command Critical Information List is not authorized for public release.

3. Contact. For issues or questions regarding public release of information contact the PAO. For issues or questions regarding OPSEC issues or concerns, contact the OPSEC Officer.