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

NAVSUPPACTNAPLESINST 5239.1
N00/N64
15 Aug 24

NAVSUPPACT NAPLES INSTRUCTION 5239.1

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

Subj: SPILLAGE OF CLASSIFIED MATERIALS

Ref: (a) DoD Instruction 8510.01 Ch-2, Risk Management Framework for Department of Defense Information Technology of 28 Jul 17
(b) DoD Instruction 8500.01, Cybersecurity of 14 Mar 14
(c) COMNAVREGEURAFSWAINST 5239.2 25 Jun 2019
(d) OPNAVINST 5239.1D, Navy Cybersecurity Program
(e) COMNAVREGEURAFSWA 5239 memo of 20 Feb 19, Interim Spillage Policy for Government Unclassified Apple iOS Devices Utilizing Mobile Device Management
(f) SECNAV-M 5210.1, Department of the Navy Records Management Program
(g) SECNAVINST 5239.19, Department of the Navy Computer Network Incident Response and Reporting Requirements

1. Purpose. This instruction establishes policies and procedures and assigns responsibilities for executing and maintaining the Cybersecurity Program requirements and implements the provisions of references (a) through (e) to the Commanding Officer (CO) of U.S. Naval Support Activity (NAVSUPPACT) Naples, Italy.

2. Background.

a. Per references (a) and (b), cybersecurity provides the measures taken by an organization to ensure the availability, integrity, authentication, confidentiality, and non-repudiation of its information and all information technology (IT) systems. Cybersecurity includes providing security of IT systems by incorporating protection, detection, and recovery capabilities.

b. Defense-in-Depth is a strategy whereby multiple layers of protection combine to establish an adequate security posture for a system and will be implemented by NAVSUPPACT Naples in accordance with reference (c). The strategy is based on the concept attacks that must penetrate multiple protection layers of the system are less likely to be successful. In addition to this layered approach, protection mechanisms are distributed among multiple locations and each component of defense within the system provides an appropriate level of robustness.

c. Department of Defense Information Network (DoDIN) operations embody incident prevention, detection, and response; a critical part of defense-in-depth. DoDIN operations synchronize the technical, operational, and intelligence assessments of the nature of a computer attack in order to defend against it.

3. Policy. Per reference (a), an electronic spillage (ES) occurs whenever classified information or controlled unclassified information (CUI) is transferred onto an IT system not authorized for the appropriate security level or not having the required CUI protection of access controls per reference (b). Examples of an ES of classified information include secret information processed on or transmitted via the non-classified internet protocol router network and TOP SECRET (TS) Special Compartmentalized Information (SCI) processed on or transmitted via the secret internet protocol router network. Examples of an ES of CUI include for official use only (FOUO) information posted to a publicly accessible website and FOUO-Law Enforcement Sensitive information forwarded to a personal e-mail address.

a. All military, civilian, and contractor personnel must follow the Department of the Navy (DoN) reporting process for ES of classified information, as well as the procedures outlined in reference (g), reporting and response procedures for ES.

b. Personnel who cause an ES, are the recipient of an ES, or are aware of an ES must take immediate action to safeguard CUI, classified material, or equipment and report the matter.

c. All cases of ES must be reported to the Command Information Systems Security Manager (ISSM) and Command Security Manager (CSM).

d. Personnel whose workstations are affected by a spillage may continue to use them once the spillage is reported and initial purging of the spillage has been accomplished in accordance with spillage process.

e. Affected laptops will remain under positive government control (e.g., left in the docking station or in the immediate possession of the user at all times while undocked) until the spillage is completely removed.

f. Personnel with government-issued mobile devices will follow the procedures in reference (e) for initial containment and continued use of the device.

g. All communications regarding the ES involving collateral TS, TS/SCI, or Special Access Program information must be transmitted via secure networks approved for information commensurate with the classification level of the report. Unclassified Naval Nuclear Propulsion Information ES must be reported via classified networks.

h. All documentation related to the spill, security inquiry, and/or ES Action Form will be maintained by the CSM and ISSM for two years per reference (f).

i. Removable storage media affected by an electronic spillage will be surrendered to the CSM immediately and stored for the higher classification level until properly sanitized. Media that cannot be sanitized will be rendered unusable and destroyed per reference (g).

4. 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).

5. 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 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 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.

RANDAZZO.JOHN.LUCIAN.1035461376 Digitally signed by RANDAZZO.JOHN.LUCIAN.1035461376 Date: 2024.08.15 11:42:45 +02'00'

J. L. RANDAZZO

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