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

BUMEDINST 5240.1
BUMED-N4
26 May 2026

BUMED INSTRUCTION 5240.1

From: Chief, Bureau of Medicine and Surgery

Subj: NAVY MEDICINE COUNTERINTELLIGENCE ACTIVITIES SUPPORTING RESEARCH, DEVELOPMENT, AND ACQUISITION

Ref: (a) DoD Instruction O-5240.24 of 8 June 2011
(b) DoD Manual 5200.01, Volume 2, DoD Information Security Program: Marking of Information, 24 February 2012
(c) DoD Instruction 5200.39 of 28 May 2015
(d) DoD Instruction 5230.09 of 25 January 2019
(e) BUMEDINST 5510.11
(f) DoD Directive 5240.06 of 17 May 2011

Encl: (1) Responsibilities
(2) Counterintelligence Support Plan Template

1. Purpose. This policy establishes the framework for coordinating counterintelligence (CI) activities in support of Research, Development, and Acquisition (RDA) programs across Budget Submitting Office (BSO) 18. This policy is rooted in the authorities and responsibilities outlined in reference (a) through (f). The primary objective is to protect critical program information (CPI) and defense-related technology from foreign intelligence exploitation, ensuring the integrity of our RDA efforts.

2. Scope and Applicability. This instruction is applicable to all BSO-18 activities that conduct, but not limited to, research, development, testing, evaluation, acquisition, and international transfers of defense-related technology to enhance the health, safety, and readiness of Navy and Marine Corps.

3. 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 found on 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 Office of the Chief of Naval Operations (OPNAV) Records Management Program (DNS-16).

4. Review and Effective Date. Per OPNAVINST 5215.17A, Bureau of Medicine and Surgery (BUMED) 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 War (DOW), 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 the 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 M-5215.1 of May 2016.

5. Information Management Control. Reports required in enclosure (1) of this instruction are exempt from reports control per Secretary of the Navy manual 5214.1 of December 2005, part IV, subparagraph 7k.

R. FREEDMAN
Acting

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/

## RESPONSIBILITIES

1. Surgeon General of the Navy and Chief, BUMED will:

a. Oversee Navy Medicine (NAVMED) CI activities supporting RDA.

b. Ensure implementation of policies and directives to support CI activities supporting RDA.

2. Director, Mission Assurance (BUMED-N45):

a. Develop and execute an overarching, integrated, policy that facilitates the Counterintelligence Support Plan (CISP) within BSO-18.

b. Advise the Surgeon General of the Navy and Chief, BUMED, or their representative, on CI vulnerabilities and requirements.

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

d. Maintain oversight of the regional security managers including BUMED Headquarters and conduct an annual assessment of the requirements set forth in reference (a).

3. Director, Headquarters (HQ) Operations (OPS), and Commanders, Naval Medical Forces Atlantic, Naval Medical Forces Pacific, and Naval Medical Forces Development Command. Ensure subordinate commands or detachments with RDA activities have a CISP.

4. BUMED HQ Activity Security Manager (ASM) and NAVMED Regional Security Managers:

a. Ensure subordinate commands or detachments with RDA activities under your purview have a CISP, per reference (a).

b. Review subordinate CISPs for compliance, execution, and maintain on file.

c. Conduct a biannual CI 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. Upon completion of the signed final assessment report, submit a copy to the immediate superior in charge ASM within 15 days of signature.

5. Medical Inspector General (MEDIG) (BUMED-N01IG). Incorporate CISP inspection line items into the existing security management checklist for inspection of this program. This checklist is managed by BUMED-N45 and maintained on the BUMED MEDIG SharePoint site.

6. Commanders and Officers in Charge of Commands Authorized to engage in RDA:

a. Ensure compliance with DOW directives and instructions related to CI and this instruction.

b. The ASM, as designated by commanding officer, is the official appointed to coordinate and oversee CI activities supporting RDA programs as described in enclosure (4) of reference (a) for the command.

c. Commands involved in export control and technology transfer refer to enclosure (3) of reference (a).

d. Coordinate the conduct of CI activities supporting international transfers and exports of defense-related technology with the supporting Defense CI Component per enclosure (3), section 4 of reference (a).

e. Ensure that RDA program managers integrate CI considerations into program planning and execution.

f. Ensure all suspected or confirmed CI incidents are reported to the local ASM and Defense CI Component Coordinating Authority.

g. Support CI risk assessments and vulnerability analyses.

7. ASM will:

a. Determine if command requires a CISP by coordinating with your local Defense CI Component. An annex must be created for those RDA programs, facilities, and cleared defense contractors (CDC) when the CI activities are unique or cannot be adequately addressed by an overarching CISP. If a CISP is required, use the template in enclosure (2) of this instruction and draft a CISP with the minimum elements of the CISP listed in appendix 2 to enclosure (3) of reference (a).

b. Coordinate completion of the command CISP with the local Defense CI Component, who will also sign the final plan per reference (a). Ensure the CISP is marked appropriately per reference (b) and reviewed annually, updated as threat conditions change, or the nature of the CI activities conducted are substantially revised, by the ASM and the local Defense CI Component.

c. Forward a copy of the final signed CISP to the echelon 3 regional security manager.

d. Follow the review and archiving requirements in appendix 2 to enclosure (3) of reference (a). If a CISP is updated or archived or retired, inform the local Defense CI Component and the echelon 3 regional security manager of the status change and forward a copy of each updated version.

e. Ensure there is evidence that the activities described in the CISP are being carried out per appendix 2 to enclosure (3) of reference (a) and enclosure (2) of reference (c).

f. Ensure there are procedures in place at the command for security and policy reviews of scientific and technical papers prior to release to the public at-large, at conferences, or at other international forums per paragraph 4 of reference (d).

g. Ensure there are procedures in place for foreign national visits, or assignments to the facility to include access to automated information systems per reference (d).

h. The CISP is a Navy Inspector General inspectable program and part of the NAVMED Security Management checklist and reviewed annually as part of the self-inspection program. This checklist is maintained on the BUMED MEDIG SharePoint site. The results of the self-inspection will be reported to the immediate superior in charge security manager, per reference (e).

i. Ensure all personnel involved in RDA activities or come in contact with or host a foreign visitor receive initial and recurring CI awareness training which should be supplemented with localized training and procedures. This training should alert them to the security and collection threats and how to and to whom they should report to should a reportable incident or event occur. Training should follow guidance set forth in references (b), (c), and (f).

8. RDA Program Managers:

a. Identify and protect CPI within their programs.

b. Cooperate with CI personnel in conducting risk assessments, vulnerability analyses, and CI activities.

c. Develop and implement security measures to mitigate CI risks.

d. Report suspected foreign collection activities to the ASM and the local Defense CI Component Coordinating Authority.

9. All Personnel Involved in RDA Activities

a. Be aware of CI threats and vulnerabilities.

b. Report any suspicious activity or contacts to the local ASM and CI personnel.

c. Comply with all security policies and procedures.

d. Participate in annual CI awareness training.

BUMEDINST 5240.1
26 May 2026

COUNTERINTELLIGENCE SUPPORT PLAN TEMPLATE
(command letterhead)

SSIC
Originator Code
DD Mmm YY

From: [Defense CI Component]
To: Commanding Officer, [Activity Requiring the CISP]

Subj: [ACTIVITY NAME] COUNTERINTELLIGENCE SUPPORT PLAN

Ref: (a) DoD Instruction O-5240.24 of 8 Jun 2011

1. A Counterintelligence Support Plan (CISP) is used to identify counterintelligence (CI) support activities required for Research, Development, and Acquisition (RDA) programs with critical program information (CPI), for DOW Component-designated research, development, test, and evaluation (RDT&E) facilities; and for cleared defense contractors (CDC) where RDA program CPI is located per reference (a).

2. Description of the facility, encompassing all RDA programs with CPI under the cognizance of an RDT&E facility, under the cognizance of a Program Executive Office, or for essential CDCs supporting the facility or RDA program where CPI is present. Refer to appendix 2 to enclosure (3) of reference (a).

a. Provide contact information for key management personnel (i.e., program manager, facility security officer, RDT&E site director, activity security manager (ASM)).

b. Include the commercial and government entity code for defense industry and CDCs affiliated with the supported facility or RDA program with CPI, if applicable.

c. Identify all RDA programs with CPI. Create an annex for those RDA programs, facilities, and CDCs when the CI activities are unique or cannot be adequately addressed by an overarching CISP.

d. Identify other activities that support the facility or program to accomplish its mission (e.g., defense industry contractors, academic institutions, Federally Funded Research and Development Centers, or test and evaluation centers–domestic and foreign).

3. Activities determination. [Refer to appendix 2 to enclosure (3) of reference (a)].

a. Specify the CI activity that will occur; when the activity will be conducted, and the assistance needed from the supported facility, program, or CDC.

b. Are reviewed with the organization's security element or the security element supporting program protection. This increases efficiency of the program protection plan, as well as other security-related actions at RDT&E facilities or CDCs.

4. Additional elements may be added as required or discussed with the local CI component.

5. The CISP will be reviewed annually, updated as threat conditions change, or the nature of the CI activities conducted are substantially revised, by the ASM and the local Defense CI Component.

Senior Defense CI Representative