



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

Canc: Jun 2025

BUMEDNOTE 5500
BUMED-N4
5 Jun 2024

BUMED NOTICE 5500

From: Chief, Bureau of Medicine and Surgery

Subj: INCLUSION OF SECURITY LANGUAGE INTO EXISTING PERFORMANCE
EVALUATION SYSTEM

Ref: (a) DoDM 5200.01 Volume 1, DoD Information Security Program: Overview,
Classification, and Declassification of February 24, 2012
(b) SECNAVINST 5510.30C

Encl: (1) Assessable Security Written Assessment Template

1. Purpose. To implement references (a) and (b) by providing additional guidance for the inclusion of security language into an existing critical element regarding continued eligibility to access classified information for civilian and military personnel assigned to Navy Medicine.
2. Scope and Applicability. This notice applies to all budget submitting office-18 supervisors of civilian and military personnel whose duties involve the creation, handling, or management of national security information, to include restricted data and formerly restricted data information when appropriate, per reference (a).
3. Action. Effective immediately, applicable personnel must comply with the requirement as detailed in paragraph 5.
4. Background. The intent is to encourage supervisors to refer security concerns as soon as they become apparent; and to provide supervisors an opportunity to annually assess their employees continued eligibility to access classified information; and for supervisors to be accountable for fulfilling their responsibilities. This is a Navy Inspector General inspectable item, per references (a) and (b).
5. Roles and Responsibilities
 - a. Civilian Human Resources (BUMED-N11). Provide guidance to supervisors of civilian personnel on the inclusion of an assessable critical element in the Department of Defense Performance Management and Appraisal Program. Sample language is listed in paragraph 6.
 - b. Supervisors of Civilian and Military Personnel
 - (1) Provide guidance on the inclusion of security language into a civilian employee's existing critical element, in regularly scheduled periodic military fitness reports or evaluations,

or a written statement (a sample written statement is in enclosure (1)), if they meet one or more of the positions or duties listed in subparagraphs 5b(1)(a) through 5b(1)(d) including, but not limited to:

- (a) Security managers and security specialists.
- (b) Personnel with a Secret Internet Protocol Router Network account.
- (c) Information system security personnel if their duties involve access to classified information and information system personnel (e.g., system administrators) with privileged access to classified system or network resources.
- (d) All other personnel whose duties include involvement with the creation or handling of classified information.

(2) This assessment can also occur in the form of a written statement as displayed in enclosure (1), per reference (b).

(3) The action taken in subparagraphs 5b(1) or 5b(2) must be annually recertified if the staff member meets one or more of the positions or duties listed in subparagraphs 5b(1)(a) through 5b(1)(d), per reference (b). This recertification can happen in the performance rating, periodic fitness report, evaluation cycle, or written statement.

c. Activity Security Managers. Maintain a list of personnel that fall into subparagraphs 5b(1)(a) through 5b(1)(d) and ensure all are recertified annually. This is a Navy Inspector General inspectable item, per references (a) and (b).

6. Sample Assessable Security Element. Verbiage to be included to meet the intent of references (a) and (b) and be used in the rating evaluation system or written statement of civilian and military personnel is provided here: “Incumbent will be held responsible for all classified material under their control and responsible for reporting any mishandling of classified material immediately to the activity security manager and their supervisor within 24 hours from time of incident.”

7. Enduring Requirement. This is an enduring requirement and will be added to the revision of BUMED Instruction 5510.11, Personnel Security Program.

8. Records Management

a. Records created as a result of this notice, regardless of format or media, must be maintained and dispositioned per the records disposition schedules located on the Department of the Navy Directorate for Administration, Logistics, and Operations, Directives and Records

BUMEDNOTE 5500
5 Jun 2024

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 notice or the records disposition schedules, please contact the local records manager or the Department of the Navy Directorate for Administration, Logistics, and Operations, Directives and Records Management Division program office.



D. K. VIA

Releasability and distribution:

This notice is cleared for public release and is available electronically only via the Navy Medicine Web site, <http://www.med.navy.mil/Directives/>

ASSESSABLE SECURITY WRITTEN ASSESSMENT TEMPLATE

DATE

MEMORANDUM FOR <COMMAND NAME> ACTIVITY SECURITY MANAGER

Subj: ASSESSABLE SECURITY STATEMENT

Ref: (a) DoDM 5200.01 Volume 1, DoD Information Security Program: Overview,
Classification, and Declassification of February 24, 2012
(b) SECNAVINST 5510.30C

1. This written statement, in lieu of security language or item to be evaluated on a performance evaluation or fitness report, meets the requirement of references (a) and (b).

2. Supervisory Responsibility. All supervisors are encouraged to refer security concerns as soon as they become apparent to your local activity security manager, annually assess your employees continued eligibility to access classified information and be held accountable for fulfilling my responsibilities, per references (a) and (b).

3. Incumbents Responsibility

a. Incumbents will be held responsible for all classified material under their control and responsible for reporting any mishandling of classified material immediately to the activity security manager and their supervisor within 24 hours from time of incident.

b. I certify that I have read and understand this Assessable Security Statement and agree to comply with the requirements that have been set forth.

c. Incumbent Signature: _____

d. Incumbent Position Title (Code): _____

4. This signed statement will expire 1 year from the date of signature and is required to be recertified on the anniversary.

5. All questions should be directed to your activity security management office.

SUPERVISOR'S NAME
Title

Copy:
Supervisor
Member