



# UNIFORMED SERVICES UNIVERSITY OF THE HEALTH SCIENCES

APR 27 2006

## SUBJECT: Information Security Program

### Instruction 5201

(SEC)

#### ABSTRACT

This Instruction implements the Uniformed Services University of the Health Sciences (USUHS) information security program. This program is established to safeguard national security information from unauthorized disclosure.

**A. Reissuance and Purpose.** This Instruction reissues USUHS Instruction 5201<sup>a</sup> to:

1. Supersede USUHS Instruction 5201, "Information Security Program," 7 April 1995.
2. Establish Policies and procedures for safeguarding national security information.

**B. References.** See *Enclosure 1*.

**C. Applicability.** This Instruction applies to all military and civilian personnel assigned to USUHS with access to classified information.

**D. Responsibilities.**

1. Vice President for Finance and Administration (VFA). The VFA is appointed by the USUHS President as the USUHS Senior Information Security Official and is responsible for the overall direction and administration of the USUHS Information Security Program

in compliance with DoD Directive 5200.1<sup>b</sup>. The VFA will:

- a. Oversee performance of the Security Manager and assure compliance with regulations and procedures pertaining to security of classified information.
- b. Assure that information prior to release to the public has been reviewed, and there will be no compromise of national security information (reference DoD Directive 5230.9<sup>c</sup>).

2. Security Division (SEC).

- a. The Director, Security Division is appointed by VFA as the security manager and the classified control officer for USUHS.
- b. The security manager will:
  - (1) Control all classified materials, which includes accountability, inventory, protection, safekeeping, and destruction.
  - (2) Establish and maintain a central Security Document Control Center for storage of classified material.
  - (3) Inspect safes, vaults and other storage containers and assure

compliance with General Services Administration (GSA) Security Standards for Storage before authorizing storage of classified documents and material outside the Central Security Document Control Center.

(4) Assure that procedures are followed to prevent unauthorized persons from gaining access to classified information.

(5) Submit an annual Information Security Program data Report (Interagency Report Control Number 0230-GSA-AN) DoD Directive 5200.1-R<sup>c</sup>.

(6) Establish and maintain a "sign-out" procedure to permit authorized users to remove classified documents from the Document Control Center.

(7) Conduct periodic inspections, perform annual inventory of all classified security documents, and report results of inventory to VFA.

(8) Maintain a current listing of employees with security clearances of Confidential, Secret and Top Secret.

(9) Review and make recommendations on all requests for security clearances.

(10) Report immediately to VFA any and all discrepancies or violations of the Security Information Program, to include compromises, losses, inappropriate requests, attempted thefts or other untoward situations.

(11) Assure that all classified documents that are transmitted to or from USUHS or picked up by a USUHS courier are in accordance with procedures outlined in DoD Directive 5200.1<sup>b</sup>.

(12) Process requests for security clearances for all assigned USUHS personnel through appropriate investigative agencies.

3. Personnel in Possession of Classified Documents (Custodian). All USUHS personnel in possession of classified materials shall:

a. Have a working knowledge of security procedures for safeguarding and protecting classified documents.

b. Assure that classified documents removed from storage are kept under constant surveillance. (*See Enclosure 2.*)

c. Determine the "need-to-know" of any other individuals before permitting them to view the contents of classified documents.

d. Attend required annual initial/ refresher security briefings.

#### **E. Procedures.**

##### Personnel Security Clearances.

1. Background. Only United States citizens will be assigned to sensitive duties or granted access to classified information unless a waiver to NCIS is approved. The person's loyalty, reliability, and trustworthiness will be determined by the adjudicator and must be such that entrusting the person with classified information is clearly consistent with the interests of national security.

2. General. The following guidelines are provided to simplify and facilitate the investigative request process:

a. Limit requests for investigation to those who are essential to current operations and clearly authorized by DoD policies. Attempt to use individuals who have already met security standards.

b. Ensure that personnel on whom investigative requests are initiated will have sufficient time

remaining at USUHS to warrant conducting an investigation.

c. Ensure that request forms and prescribed documentation are properly executed.

d. Promptly notify the USUHS Security Manager if investigation is no longer needed.

e. Limit access through strict "need-to-know."

### 3. Request for Personnel Security Clearance.

a. A request for a security clearance for USUHS personnel (military or civilian) shall be made in memorandum form. The request will provide adequate justification for requiring a security clearance in conformance with this Instruction. The request will be signed by the Department Chairperson/Activity Head.

b. The Security Manager will investigate the request and assure that

the level of clearance requested is appropriate and that a "need-to-know" exists. In the event the SEC believes that the requested level of clearance is higher than required, or that a "need-to-know" does not exist, the request will be forwarded to the VFA for approval/disapproval.

c. The SEC will take action on all requests to obtain a security clearance for the individual in accordance with procedures outlined in this Instruction and in DoD Directive 5200.2R<sup>d</sup>.

(1) A certification of military personnel will be accomplished by access roster published by the USUHS Security Office.

**F. Effective Date.** This Instruction is effective immediately.



Charles L. Rice, M.D.  
President

Enclosures:

1. References
2. Security Procedures

**REFERENCES**

- (a) USUHS Instruction 5201, "Information Security Program," dated April 7, 1995 (hereby cancelled)
- (b) DoD Directive 5200.1, "DoD Information Security Program," dated December 13, 1996
- (c) DoD Directive 5200.1-R, "Information Security Program Regulation," dated January 14, 1997
- (d) DoD Directive 5200.2-R, "DoD Personnel Security Program," dated January, 1987
- (e) DoD Directive 5230.9, "Clearance of DoD Information for Public Release," dated April 9, 1996
- (f) Executive Order 12958, "Classified National Security Information," dated April 7, 1995

## SECURITY PROCEDURES

### 1. Downgrading and Declassification.

Downgrading and declassification action on a document shall be completed by the USUHS Security Division.

### 2. Safekeeping and Storage.

a. Classified material will be stored only under conditions adequate to prevent authorized persons from gaining access. All storage containers shall be approved by the Security Division.

b. Classified documents received after non-working hours at USUHS will be delivered to the National Naval Medical Center (NNMC) Communications Center for safekeeping.

c. No funds, weapons, medical items, controlled drugs, precious metals, or other items susceptible to theft, will be stored in containers containing classified material. The President, USUHS, may waive this restriction in emergencies when requested by the Security Division if acceptable storage equipment is not available.

### 3. Combinations to Classified Containers.

a. Request for changing combinations for security containers will be submitted to the Security Division, using a USUHS Form 5335, "USUHS Service/Work Request."

b. Standard Form 700, "Security Container Information," will be used to identify personnel who have knowledge of the contents of the security containers. Standard Form 700 will be positioned on the inside of each top drawer of each security container. The number of persons with knowledge of security combinations will be limited to those necessary for operational efficiency and will not exceed three. (The personnel

must meet security clearance requirements.) At least one of the named individuals will be contacted in the event the security container is discovered unsecured during non-duty hours.

### 4. Responsibilities of Users.

a. Users of classified information will be responsible for providing protection and accountability for such information at all times and for locking classified information in appropriate security containers when it is not in use or not under direct supervision of authorized persons. Users will follow procedures to ensure that unauthorized persons do not gain access to classified information.

b. Classified material shall not be removed from USUHS without prior approval of the Security Manager. Under no circumstances will individuals be authorized to retain classified information overnight in their residences.

### 5. Care During Working Hours.

a. Access to work areas must be controlled at all times where classified material is being used. This may be accomplished by receptionists, secretaries, or electro-mechanical equipment. When it becomes necessary for receptionists or secretaries to leave their desks, a substitute to control classified material will be provided at every instance.

b. All visitors, messengers, and couriers must be identified, their business stated, their "need-to-know" verified and security clearance verified through the USUHS Security Division before access is granted.

c. All uncleared visitors (including maintenance and telephone personnel) must be under continuous escort or surveillance while in the presence of classified information or material.

d. When protecting classified documents, the custodian will:

(1) Cover or turn face down any classified papers or material on desks or work area.

(2) Cause classified discussions to be terminated for the duration of the uncleared visit.

(3) Affix classified document cover sheets to documents when they are removed from security containers.

(4) Classified information will not be discussed on commercial telephones. The use of codes or attempts to talk around classified subjects is prohibited.

(5) Turn over any unsecured and unattended classified material to USUHS Security Division for appropriate action. The finding of such material constitutes a security violation and will be reported by the USUHS Security Division, DoD Directive 5200.1<sup>b</sup>.

(6) Annotate on SF-702, "Security Container Check Sheet," whenever a Security Container is opened or closed.

#### 6. End-of-Day Security Checks.

a. At the close of each working day, all USUHS personnel will:

(1) Inspect their immediate work area for classified material, paying particular attention to the contents of desks, in-and-out trays, and waste containers.

(2) Survey the general work area to ensure that no classified material remains unsecured.

(3) Place classified notes, carbon paper, rough drafts, and similar

classified papers in burn bags and store in appropriate security containers.

(4) Remove and secure typewriter ribbons or portions of typewriter ribbons that have been used to prepare classified material. Miniature memory storage units will be removed and secured from typewriters so equipped.

(5) Return classified documents, correspondence, or related classified information to proper security containers.

(6) Secure the security containers when their contents are no longer needed for the day. Annotate SF-702 at the end of each work day.

b. At least one individual will be designated on a rotating or permanent basis to be responsible for double checking each office/laboratory to ensure that classified materials and security containers have been properly secured before leaving the work area.

(1) Form 701 "Activity Security Check List," will be used as a record for double checking the office/laboratory, and will be placed at the primary exit.

(2) When the office is occupied after duty hours, the last person leaving the office assumes responsibility for double checking and securing the area.

c. When notified that a security container has been left unattended, those responsible for the container will be required to check the contents of the container for indications of tampering or removal of materials (inventory of container). During non-duty hours, the same procedure will apply.

#### 7. Reproduction Controls.

a. All classified documents, if approved for reproduction by the Security Manager, will be reproduced by

the requesting official in the Security Manager's office area.

b. Reproduction of documents containing classified information will be held to the minimum necessary to accomplish operational objectives and any stated prohibition against reproduction will be strictly observed,

c. All copies of classified documents reproduced for any purpose, including those incorporated in a working paper, are subject to the same controls prescribed for the document from which the reproduction is made.

#### 8. Accountability and Control.

a. Receipt for classified material. AF Form 310, "Document Receipt and Destruction Certificate," is the only form approved for transfer of classified accountable material at USUHS. A supplement receipt, such as SD Form 188, "Request for Certification of Destruction of Classified material," may be used when transmission or destruction involves multiple documents.

b. When an inventory discloses that classified materials are missing or unaccounted for, the USUHS Security Manager will be notified immediately.

c. The USUHS Security Manager will be responsible for receiving, processing, logging, transmitting and accounting for all classified documents within USUHS.

d. USUHS classified document users will establish administrative procedures for controlling classified material within their respective areas. Inter-departmental transfer of documents will be accomplished by the Security Manager only.

#### 9. Disposal and Destruction.

a. The Security Manager has overall responsibility for the timely and

complete destruction of all classified material.

b. Classified material will be placed in standard red-striped burn bags and transported to the Pentagon Central Destruction Facility by USUHS Security Personnel or shredded in the Security Office.

c. Only government vehicles will be used to transport material to the destruction facility.

d. Records of destruction of Secret and Confidential information are not required except for NATO Secret and some limited categories of specially controlled Secret information. When records of destruction are used for Secret information, only one cleared person has to sign the AF Form 310 or SD Form 188.

e. Under emergency destruction conditions, all documents deemed unnecessary will be destroyed as quickly as possible using the paper shredder located in the Security Office, Room UP-001.

10. Security Education. Supervisors will include proper procedures for the protection of classified materials and information in office orientation for newly assigned personnel. The USUHS Security Manager will provide instructions to supervisors and custodians as necessary or requested. Newly assigned persons will not be made solely responsible for securing classified materials or offices until they have completed security orientations and training designed to familiarize them with proper storage and office closing procedures.

a. Initial/Refresher Briefings. In addition to initial security orientations, periodic security training for incumbent personnel will be tailored to the needs of

experienced personnel while including essential elements of DoD Directive 5200.1-R<sup>c</sup>. Annual security refresher briefings will be arranged by the Security Division. Attendance is mandatory for all custodians.

b. Foreign Travel Briefings. USUHS faculty, staff members, residents, fellows, and students contemplating travel in foreign countries under the conditions described in DoD Directive

5200.1-R<sup>c</sup> will be briefed by USUHS security personnel. In addition, medical and GSN students traveling in foreign countries will coordinate their travel requests with their Office of the Commandant (First Sergeants, Commanders); School of Medicine graduate students, residents, and fellows will coordinate their travel requests with their military and academic supervisors.