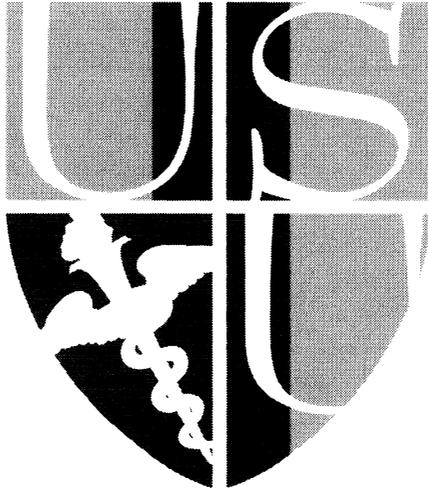


**USUHS
INSTRUCTION
5203**





UNIFORMED SERVICES UNIVERSITY OF THE HEALTH SCIENCES



SUBJECT: Uniformed Services University of the Health Sciences (USUHS) Civilian Personnel Security and Suitability Investigative Program

Instruction 5203

(SEC)

ABSTRACT

SEP 5 2006

This Instruction provides policy and guidance regarding the Uniformed Services University (USU) Civilian Personnel Security and Suitability Investigative Program. Included in this Instruction are new procedures for processing investigations.

A. Reissuance and Purpose. This Instruction reissues USUHS Instruction 5203^a, implements 5 CFR, Part 731^b, 5 CFR, Part 736^c, and Executive Order 10450^d, and assigns responsibilities to the USUHS Security Division (SEC) in accordance with 5 CFR, Part 731^b, USUHS Instruction 5201^e, DoD Regulation 5200.2-R^f, 5 CFR, Part 732^g, and DoD Directive 5105.45^h. It prescribes procedures for administering the Personnel Security Program (PSP) and the Civilian Personnel Suitability Program (CPSP).

B. References. See *Enclosure 1*.

C. Applicability. The provisions of this Instruction apply to all USU civilian employees.

D. Definitions. See *Enclosure 2*.

E. Policy.
The appointment of any civilian officer or employee in the Government shall be

made subject to investigation in accordance with 5 CFR, Part 736^c, Executive Order 10450^d, USUHS Instruction 5201^e, DoD Regulation 5200.2-R^f, and 5 CFR, Part 732^g. The scope of the investigation will be determined by the sensitivity level of the position. Seasonal or temporary employees who are employed in a non-sensitive position and whose employment does not exceed an aggregate of 120 days are not subject to investigation. If deemed necessary by the USU, a National Agency Check (NAC) may be conducted in accordance with DoD Regulation 5200.2-R^f.

F. Responsibilities.

1. The President, USU shall ensure that the PSP and CPSP are operational.

2. The Vice President, Finance and Administration (VFA) shall:

- a. Oversee the USU PSP and CPSP.
- b. Ensure all personnel within the USUHS are aware of the provisions of this Instruction.

3. Department Chairs/Activity Heads shall designate the position sensitivity level for each position under their direction, in accordance with applicable DoD and Office of Personnel Management (OPM) regulations.

4. The Civilian Human Resources (CHR) shall:

- a. Determine job qualifications in coordination with the appropriate department chair or activity head.
- b. Determine the employee's suitability for continued employment. If the employee is found unsuitable, based on disqualifying factors from OPM investigative results, CHR, in coordination with the USU Security Officer and the VFA, with the approval of the President, USU, will institute adverse action procedures to separate the employee from his/her position.

5. The Security Officer shall:

- a. Assist the USU Departments and Activities in determining the position sensitivity for all positions within the USUHS, and provide recommendations to the VFA for final decisions over designations.

b. Prescreen applicants/employees and initiate background investigations as appropriate.

c. If applicant is a Foreign National (FN) being assigned to a sensitive position, the security officer will notify CHR of the waiver requirements. (*See Enclosure 3.*)

d. Ensure Departments and Activities are aware of the current security measures in place to preclude FNs from accessing classified and sensitive information. (*See Enclosure 4.*)

e. Evaluate investigative results received from OPM for suitability determination and advise CHR, the VFA, and when appropriate, the President, USU of any noted disqualifying issues.

f. Provide initial/annual security briefings and debriefings for all USU personnel. Each briefing is described in *Enclosure 5.*

G. Procedures. *See Enclosure 6.*

H. Effective Date. This Instruction is effective immediately.



Charles L. Rice, M.D.
President

Enclosures:

1. References
2. Definitions
3. Memo Request for Suitability Clearance
4. Briefings
5. Procedures

REFERENCES

- (a) USUHS Instruction 5203, "Uniformed Services University of the Health Sciences (USUHS) Personnel Security and Suitability Programs," dated April 19, 1996 (hereby cancelled)
- (b) 5 Code of Federal Regulations, Part 731, "Personnel Suitability"
- (c) 5 Code of Federal Regulations, Part 736, "Personnel Investigations"
- (d) Executive Order 10450, dated April 27, 1953
- (e) USUHS Instruction 5201, "Information Security Program," dated April 7, 1995
- (f) DoD Regulation 5200.2-R, "Personnel Security Program," dated January 1, 1987
- (g) 5 Code of Federal Regulations, Part 732, "National Security Positions"
- (h) DoD Directive 5105.45, "Uniformed Services University of the Health Sciences (USUHS)," dated March 9, 2000

DEFINITIONS

1. **Adverse Action.** A removal from employment, suspension from employment of more than 14 days, reduction in grade, reduction in pay, or furlough of 30 days or less.

2. **Interim Security Clearance.** A security clearance that is granted on a temporary basis, pending completion of the full investigative requirements.

3. **National Agency Check (NAC).** A personnel security investigation that consists of a records review of certain national agencies, as prescribed in DoD Regulation 5200.2-R^f, including a technical fingerprint search of the Federal Bureau of Investigation (FBI) files.

4. **National Agency Check and Inquiries (NACI).** A personnel security investigation conducted by OPM that combines the NAC with written inquiries to law enforcement agencies, former employers and supervisors, references, and schools.

5. **Periodic Reinvestigation (PR).** An investigation conducted every five or ten years for the purpose of updating a previously completed background or special background investigation on individuals occupying sensitive and public trust positions.

6. **Security Clearance.** A determination that an individual is eligible, under the standards outlined in DoD Regulation 5200.2-R^f, for access to classified information. The type of investigation depends on the designated position

sensitivity level. Position investigative requirements are as follows:

a. **Critical-Sensitive Positions (Position Sensitivity Designator "3").** Nominees for Critical-Sensitive positions must receive a favorable Single Scope Background Investigation (SSBI) that meets the scoping requirements in DoD Regulation 5200.2-R^f before being appointed.

b. **Non-critical-Sensitive Positions (Position Sensitivity Designator "2").** Nominees for Non-critical-Sensitive positions must have a favorable NAC portion of an NACI completed before appointment. Nominees for these positions who have not had an NACI investigation shall be required to submit the forms within 10 working days to SEC.

c. **Non-sensitive Positions (Position Sensitivity Designator "1").** Nominees for Non-sensitive positions that do not require a security clearance shall be required to have a NACI. The NACI, which is conducted by OPM, is the fundamental investigation for determining an individual's suitability for Federal civilian employment.

7. **Suitability.** Fitness or eligibility for employment or continued employment of an individual in the federal service who is expected to reasonably promote the efficiency of the federal service.

8. **Sensitive Position.** Any position, so designated within the DoD, in which the occupant could bring about, by virtue of the nature of the position, a materially adverse effect on the national security. All civilian positions are either critical-sensitive, non-critical-sensitive, or non-sensitive.

9. **SSBI.** Replaces the Background Investigation (BI) and the Special Background Investigation (SBI).

**U.S. Citizenship Requirement Waiver Procedures for Persons
Nominated to Occupy DoN Sensitive Positions**

SENSITIVE POSITIONS WITHOUT INFORMATION TECHNOLOGY (IT) DUTIES

1. Requests for a waiver of the U.S. citizenship standard for persons nominated to occupy DON sensitive positions without IT duties will include:
 - a. The full identity of the applicant and the applicant's country of origin.
 - b. The original completed investigation request forms (SF 86, all releases and fingerprint cards) which CNO (N09N2) will review and forward to OPM, as appropriate.
 - c. A copy of the OPM employment approval or other documented authority under which the offer of employment to a non-U.S. citizen is permitted, indicating whether the proposed employee will be hired as excepted service, consultant, temporary employee, seasonal or other.
 - d. Documentation identifying the applicant's immigration status, alien residency and/or other visa status.
 - e. A detailed justification of the compelling reasons requiring assignment (to include special expertise) signed by the commanding officer.
 - f. A detailed description of the sensitive duties to be performed or sensitive information to be accessed, including all IT system accesses required.
 - g. A detailed description of the security measures and mechanisms in place to preclude the individual from having access to classified information and/or controlled unclassified information (CUI), and to address the security risks presented by NCIS during the country-specific counterintelligence briefing. Commands should consult with Navy IPO for additional guidance regarding foreign disclosure of CUI.
2. CNO (N09N2) will review and coordinate the request with the appropriate authorities to determine if sufficient justification exists and if adequate security protections are in place. If the request conforms to employment and security requirements and is sufficiently consistent with the interests of national security, USU will be advised and the request for investigation will be forwarded to OPM. Upon completion, investigations conducted on non-U.S. citizens occupying sensitive positions will be forwarded to CNO (N09N2) for the required personnel security determination. USU will then be advised of the adjudicative results.

Security Measures to preclude Foreign Nationals Access to USU Unclassified Information and Network Policy

1. **Purpose:** Establishes policy for Foreign Nationals (FN) nominated to occupy sensitive positions within the USU.
2. **Scope:** This policy applies to FN's working in sensitive positions and their ability to access information, their user accounts, and user level privileges. Additional requirements must be met for an FN to have administrator privileges. In addition, this policy only applies to unclassified information and network. The USU does not maintain any classified information or networks, however, FN access to classified networks or controlled unclassified information requires additional authority delineated within DOD 5200.2R. This policy is intended to reaffirm and consolidate existing higher authority policy as it applies to the USU. This policy applies to Foreign National Employees, Foreign National Service Members and DOD Foreign National Contractors.
3. **Policy:** USU FNs are identified by a red strip on the USU ID Badge and Common Access Card (CAC). FNs will be granted access to unclassified, non-sensitive information and networks provided the following are met.
 - a. Each FN is visually identified with a red stripe on their USU badge as well as their Common Access Card.
 - b. Badges are to be worn at all times at the USU. They must be worn on the front portion of the body, with the picture facing forward for easy identification.
 - c. During the initial and annual security briefs, all USU personnel (Military, Civilian, and Contractor) are made aware of the identifying badge requirements.
 - d. FN users on the unclassified USU network must have their FN affiliation displayed as part of their e-mail address.
 - e. Auto e-mail signature blocks will be used and will include foreign individual's name, nationality, duty description, and organization assigned. Format example: Doe, John WG CDR, United Kingdom-FLO, Fleet Commander (Ref D). This address must also be reflected in the FNs CAC e-mail address.
 - f. FN will not be granted access to enclaves protecting controlled unclassified information unless all information contained on the enclave has been approved for disclosure to that foreign national's parent government by an approved disclosure authority (References B and D).
 - g. Prior to access to USU network, each FN user will sign the user agreement that includes the following (References B and D).
 - (1) Acknowledging information and information security policies, procedures, and responsibilities.

Enclosure 4

- (2) Consequences of not adhering to security procedures and responsibilities.
 - (3) For e-mail accounts, the user name will include individual's nationality to preclude inadvertent disclosure of controlled unclassified information not authorized to foreign nationals.
 - (4) Remote access and GroupWise Web Access privileges are at the discretion of the USU. If remote access is granted, the DoD PKI software certificate issued will reflect the digraph "FN" in the generational field of the distinguished name.
4. This policy does not remove the obligation of owners of unclassified export controlled technical data from ensuring that data is safeguarded IAW the International Traffic in Arms Regulation (22 CFR 121-128) or the Export Administration Regulations.
 5. This policy will remain in effect until canceled or replaced by higher guidance.

Security Briefings/Debriefings

Personnel who have access to classified information will refer to USUHS Instruction 5201^e for the specific briefings. Required briefings are:

1. **Initial Security Briefing** - All USU personnel are required to have an initial security briefing and to read and sign the "Nondisclosure Agreement," (SF-312), prior to receiving access. If an individual declines, action will be taken to deny or revoke the security clearance.

2. **Annual Security Briefing**. All USU personnel are required to attend an annual security briefing. This briefing will cover Personnel Security and investigative requirements for USU personnel. It will also cover Physical Security and the badge requirements:

Purple Stripe - US citizen government employee.

Red Stripe – Non-US citizen government employee or contractor.

Green Stripe - US citizen Contractor.

3. **Debriefing** - Upon termination of a clearance, a Security Termination Statement will be executed and all classified information will be returned to the SEC Office under the conditions outlined in DoD Regulation 5200.2-R^f, paragraph 9-204.

PROCEDURES

1. Criteria for Security Designation of Positions. Each civilian position within the DoD shall be categorized, with respect to security sensitivity, as either non-sensitive, non-critical-sensitive, or critical-sensitive.

a. The criteria to be applied are:

(1) Critical-sensitive:

(a) Access to Top Secret information.

(b) Development or approval of plans, policies, or programs that affect the overall operations of the DoD or of a DoD Component.

(c) Investigative and certain investigative support duties, the issuing of personnel security clearances or access authorizations, or the making of personnel security determinations.

(d) Fiduciary, public contact, or other duties demanding the highest degree of public trust.

(e) Duties falling under Special Access programs.

(f) Category I automated data processing (ADP) positions.

(g) Any other position so designated by the head of the Component or designee.

(2) Non-critical-sensitive:

(a) Access to Secret or Confidential information.

(b) Security police/provost marshal-type duties that involve the enforcement of law, and security duties that involve the protection and safeguarding of DoD personnel and property.

(c) Category II ADP positions.

(d) Duties involving the design, operation, or maintenance of intrusion detection systems deployed to safeguard DoD personnel and property.

(e) Any other position so designated by the head of the Component or designee.

b. All other positions shall be designated as non-sensitive.

2. Civilian Employees and Prospective Civilian Employees - Suitability for Federal Employment.

a. Position Sensitivity Categories:

(1) Nominees for **Non-sensitive positions** must have an investigation initiated within three working days after appointment if the appointment is:

(a) **Approved for more than 120 days of employment.** When an employee's appointment exceeds 120 days, in either a single-continuous or series of appointments with the USUHS, he/she will be fingerprinted and will complete either an SF-85, "Questionnaire for Non-sensitive Positions" or an SF-85P, "Questionnaire for Public Trust." The SEC will forward the required forms to OPM's Federal Investigations Processing Center, Boyers, PA, or

(b) **Approved for less than 120 days of employment.** If an appointment is for less than 120 days of employment, within a year time-period of the starting date, appointees do not require an investigation.

Summer hires and temporary employees require a favorably adjudicated NAC through Defense Investigative Service (DIS).

(2) Nominees for **Critical-Sensitive positions** must have completed a favorably adjudicated SSBI prior to appointment at the USUHS. In an emergency where a delay in appointment would adversely affect the Agency, the following exceptions apply:

(a) A waiver for an appointee to a Critical-Sensitive position may be approved by the President, USUHS only after completion of the NAC portion of the SSBI, or completion and favorable adjudication of a previous NACI, NAC, or Entry National Agency Check (ENTNAC), or

(b) A request for waiver must include justification from the Department Chair or Activity Head and be approved by the President, USUHS and the appropriate Dean prior to submission to the DON/CAF.

(3) Nominees for **Non-critical-Sensitive positions** must have completed a favorable NACI conducted by OPM prior to appointment at the USUHS. In an emergency where a delay in appointment would adversely affect the Agency, the following exceptions apply:

(a) A waiver for a nominee to a Non-critical-Sensitive position may be approved by the President, USUHS only after the NACI has been initiated, or

(b) In an emergency, and with concurrence from the Director, DON/CAF, sensitive positions may be occupied by individuals not initially meeting the minimum investigative requirements for entry on duty.

b. Administrative Procedures for Sensitive Positions and Clearances:

(1) All USUHS DoD civilian employees whose positions require a clearance and/or who occupy a sensitive position must have the appropriate investigation completed before they can be brought on board or be granted access to classified information. The USUHS SEC Officer will grant access once the DON/CAF determines the person is eligible for a clearance and/or occupancy of a sensitive position.

(2) When the SEC Division determines that it is in the interest of national security to deny or revoke a security clearance for access to classified information and/or eligibility to occupy a sensitive position, the case will be forwarded to DON/CAF for approval. An interim security clearance is issued by USUHS SEC for a period of 90 days.

(3) If OPM finds that an investigation has produced suitability-related issues that require adjudication, examiners will mark the case with a suitability level designator as appropriate. The OPM will then return the case to DON/CAF if the case is critical-sensitive or non-critical-sensitive, and to the USUHS SEC Division if non-sensitive, for final processing and adjudication of the case.

3. Adverse Actions and Appeals.

a. If, based on an evaluation of the issues produced by the investigation and the advice of USUHS SEC and/or DON/CAF, CHR determines that the employee's continued employment with the USUHS will not promote the efficiency of the service, CHR, in coordination with the USUHS Security Officer and the VFA, with the approval of the President, USUHS will institute adverse action procedures to separate the employee from his/her position.

Enclosure 6

b. Employees who, based on a suitability determination have been separated from employment by either the USUHS or OPM, have a right of appeal in accordance with the time limits and procedures to the Merit Systems Protection Board (MSPB). This action does not apply to Excepted Service positions.

c. If the position is critical-sensitive or non-critical-sensitive, or requires a clearance, the DON/CAF shall provide the employee with a Letter of Intent (LOI) delineating the reasons for which the action is being taken.

This statement will be as comprehensive and as detailed as possible, without compromising the source of confidentiality, as afforded by the provisions of the Privacy Act of 1974 and national security. The employee has 10 days to acknowledge receipt of the LOI in writing to the DON/CAF through USUHS SEC. The employee has 30 days in which to provide his/her written rebuttal, which may include any mitigating information, through the SEC Office to DON/CAF