# UNIFORMED SERVICES UNIVERSITY OF THE HEALTH SCIENCES

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

JUN 0 4 2018

# Instruction 5203

(SEC)


ABSTRACT

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, September 5, 2006, in accordance with regulatory updates.

**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, Parts 1400, 731, 732, Executive Order 10450, USUHS Instruction 5203, and DoDM 5200.02. 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 180 days are not subject to investigation unless deemed necessary by the agency. If deemed necessary by the USU, a National Agency Check (NAC) may be conducted in accordance with DoDM 5200.02.

**F. Responsibilities.**

1. The President USU:

a. Shall ensure that the Personnel Security Program (PSP) and Civilian Personnel Security Program (CPSP) are operated in accordance with Office of Personnel Management (OPM) and DoD regulations, polices, and procedures. As such, the President has designated the Security Officer as responsible for the direction, overall management, functioning, and administration of the USU PSP

b. Has the authority to determine the position sensitivity for all positions within USU.

c. Has delegated the authority to determine position sensitivity as follows:

1) The Security Office shall make the determination of position sensitivity; and

2) The Assistant Vice President (Chief of Staff) shall make the final determination when there is a dispute regarding the appropriate position sensitivity.

2. Supervisors:

a. Shall determine the duties and responsibilities of position descriptions (PD) within their organization in consultation with CHR.

b. Initiate requests for reconsideration of position sensitivity determinations to the Assistant Vice President (Chief of Staff) for review when there is a concern regarding a position sensitivity determination.

3. Civilian Human Resources (CHR) shall:

a. In coordination with supervisors, ensure the accuracy of position descriptions (PD) and determine job qualifications.

b. Forward PDs to the Security Office for a position sensitivity determination.

c. Forward PDs with completed position sensitivity designation records (PDR) to the Department of Navy, Office of Civilian Human Resources (OCHR), Silverdale, WA, to maintain. Advises the appropriate department supervisor when there is change in the position sensitivity of a current position based on the position sensitivity determination by security.

d. Provide recommendations on adverse actions concerning an 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 Chief of Staff, with the approval of the President, USU, will institute adverse action procedures to separate the employee from his/her position.

e. Forward received completed Certifications of Investigations (COI) to OCHR to place in agency employees Official Personnel Files (OPF).

4. Security Office shall:

a. Determination the position sensitivity for all positions within USU based on the duties and responsibilities of the position using the OPM Position Designation Automated Tool (PDT) and the OPM suitability handbook for accuracy in accordance with applicable OPM and DoD policies, regulations, and requirements. Forward PDs along with position sensitivity designation determinations to CHR.

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

c. Ensure Departments and Activities are aware of the current security measures in place to preclude non-United States citizens from accessing classified and sensitive information. Non-United States citizens will not be approved to occupy positions requiring a national security clearance.

d. Determine suitability and/or evaluate investigative results received from OPM for suitability determination and advise CHR, the Chief of Staff, and when appropriate, the President, USU, of any noted disqualifying issues.

e. Provide initial/annual security briefings and debriefings for all USU personnel.

f. Advises employees of the appropriate background investigation they must complete when the position sensitivity designation of the current position they occupy is changed based on the position sensitivity designation determination.

g. Consults with the Assistant Vice President (Chief of Staff), and the USUHS President, if necessary, on submitted requests for reconsideration of a position sensitivity determination.

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

Richard Thomas MD, DDS, FACS
President

Enclosures:
1. References
2. Definitions
3. Briefings
4. Non US Citizens/Limited Access Authorization (LAA)
5. Pre-employment Processing of Employees

## REFERENCES

A. USUHS Instruction 5203, "Uniformed Services University of the Health Sciences (USUHS) Personnel Security and Suitability Programs," September 8, 2005 (cancelled)

B. DoD Manual 5200.02, "Procedures for the DoD Personnel Security Program (PSP)," April 3, 2017.

C. Title 5, Code of Federal Regulations, Part 1400 "Designation of National Security Positions."

D. Title 5, Code of Federal Regulations, Part 731, "Suitability."

E. Title 5, Code of Federal Regulations, Part 732, "National Security Positions."

F. Title 32, Code of Federal Regulations, Part 156, "Department of Defense Personnel Security Program (PSP)."

G. Executive Order 10450, "Security Requirements for Government Employment, April 27, 1953, as amended.

H. Executive Order 13467, "Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information," June 30, 2008.

## DEFINITIONS

1. **Access**. The ability and opportunity to obtain knowledge of national security information. An individual may have access to national security information by being in a place where such information is kept, if the security measures that are in force do not prevent the individual from gaining knowledge of such information.

2. **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.

3. **Interim Security Clearance.** A security clearance based on the completion of minimum investigative requirements, which is granted on a temporary basis, pending the completion of the full investigative requirements.

4. **Limited Access Authorization**. Authorization for access to confidential or secret information granted to non-U.S. citizens and immigrant aliens, limited to only that information determined releasable by a U.S. Government designated disclosure authority to the country of which the individual is a citizen, in accordance with DoDD 5230.11. Access is necessary for the performance of the individual's assigned duties with the military or a federal agency and is based on favorable adjudication of a 10-year scope SSBI. An LAA will not be granted for Critical/TS/T5 level access.

5. **National security.** Refers to those activities which are directly concerned with the foreign relations of the United States, or protection of the Nation from internal subversion, foreign aggression, or terrorism

6. **National Agency Check (NAC).** A personnel security investigation that consists of a records review of certain national agencies, as prescribed in DoD Regulation 5200.02-R, including a technical fingerprint search of the Federal Bureau of Investigation (FBI) files.

7. **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.

8. **Need-to-know.** A determination made by a possessor of classified information that a prospective recipient, in the interest of national security, has a requirement for access to, knowledge, or possession of the classified information in order to perform tasks or services essential to the fulfillment of an official U.S. Government program. Knowledge, possession of, or access to, classified information shall not be afforded to any individual solely by virtue of the individual's office, position, or security clearance.

9. **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.

10. **Security Clearance.** A determination that an individual is eligible, under the standards outlined IAW DoD and Federal regulations for access to classified information.

11. **Security Professional.** U.S. Government military or civilian personnel (including but not limited to security managers and special security officers) whose duties involve managing or processing personnel security actions relating to the DoD PSP.

12. **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.

13. **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.

## Security Briefings/Debriefings

Required briefings are:

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

2. **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, paragraph 9-204.

3. **Annual Security Briefing** - All USU personnel are required to review an annual security briefing. This briefing will cover Personnel Security and investigative requirements for USU personnel.

Personnel who have access to classified documents will refer to USUHS Instruction 5201 for that specific information.

## Non US Citizens and Limited Access Authorization (LAA)

**Only U.S. citizens are eligible for access to classified information.**

However, compelling reasons may exist for granting access to classified information to a non-U.S. citizen. An LAA enables a non-U.S. citizen to have limited access to classified information, but the LAA is **not** a national security eligibility. An LAA may be granted, in rare circumstances, when:

1) A cleared or clearable U.S. citizen is not readily available or does not possess the skills or expertise required.

2) The non-U.S. citizen possesses unique skills or expertise needed to support a specific U.S. Government requirement involving access to classified information.

**Authorized Access Levels**:

LAAs may be granted only at the Secret and Confidential levels. Limited access to Secret and Confidential information may be granted following completion of the SSBI.

**Unauthorized Access Levels:**

An LAA granted under the provisions of DoDM 5200.02 is not valid for access to:

1) Top Secret information.

2) Restricted data (RD) or formerly restricted data.

3) Information that has not been determined releasable by a U.S. Government designated disclosure authority to the country (ies) of which the individual is a citizen.

4) Communications security (COMSEC) information.

5) Intelligence information.

6) Information for which foreign disclosure has been prohibited in whole or in part.

7) Information provided to the U.S. Government in confidence by a third party government and classified information furnished by a third party government.

## USUI 5203

## Pre-employment Processing of Employees

This provides guidance on pre-employment processing of applicants prior to entrance on duty (EOD) with the University. The provisions apply to the pre-employment processing of all USUHS Federal civilian employees.

**General Procedures:**

1. The candidate is selected by the designated official.

2. The Civilian Human Resources (CHR) or the Department of Navy, Office of Civilian Human Resources (OCHR), as applicable, will conduct and complete candidate qualification pre-screens prior to EOD.

3. If all qualification requirements are met, CHR or OCHR will make tentative job offer and issue Form 306 (Declaration of Federal Employment) and on boarding package to the candidate.

4. The candidate accepts the position and returns the completed Form 306 and the other on-boarding documents to CHR or OCHR.

5. The CHR reviews the Form 306 for completeness. (**Note**: If any derogatory information is reflected on the Form 306, the CHR Specialist will immediately notify the Chief, Staffing and Classification Division, and the CHR Director, and the document will be sent to the Security Director for review and coordination. No derogatory information regarding applicants will be shared with personnel not involved in the pre-screening or adjudicative process including the hiring manager)

6. The CHR completes USUHS Form 5203(Investigation Requirements for Employment) and forwards Form 5203, Form 306, the candidate's resume/CV, and position description (PD) to the USUHS Security Department (SEC) for review and processing. The CHR will also notify the applicant that his/her Form 306 will be submitted to SEC to begin processing their security background investigation.

7. If applicable, CHR will initiate/coordinate additional pre-employment requirements (drug testing, physical examination, etc.).

8. Security process is as follows:

a. The CHR will advise the applicant that his/her Form 306 has been submitted to SEC to begin processing their security background investigation. He or she will be contacted by a security representative and advised of the process for completing their security questionnaire. Once the security process is reflected as open in the security system, the Joint Personnel Adjudication System (JPAS), the Security Department will advise CHR, and a CHR representative will contact the applicant to establish a start date.

b. The Security staff, via email, will contact the applicant and send instructions to them on the process for completing his or her security background questionnaire in the security system (JPAS).

c. Security will allow the applicant 14 days to complete the investigation in the security system and provide information on finger printing options.

d. Once the packet is reviewed for accuracy and completeness (eQIP packet, signature sheets, Form 306, and finger prints), the security staff will release the information to the Office of Personnel Management (OPM). **Note**: This process could take OPM 30 to 60 days to complete depending on the level of the background investigation required.

e. Once the investigation reflects as open in JPAS, Security will return the completed Form 5203 to CHR.

9. Upon completion of all pre-employment requirements and receipt of the authorized Form 5203 from SEC, CHR will make the formal job offer and establish an EOD date.

10. The applicant EODs and CHR conducts employee orientation.

11. CHR or OCHR, as applicable, processes the personnel action in the human resources system (DCPDS) within 5 workdays of EOD.