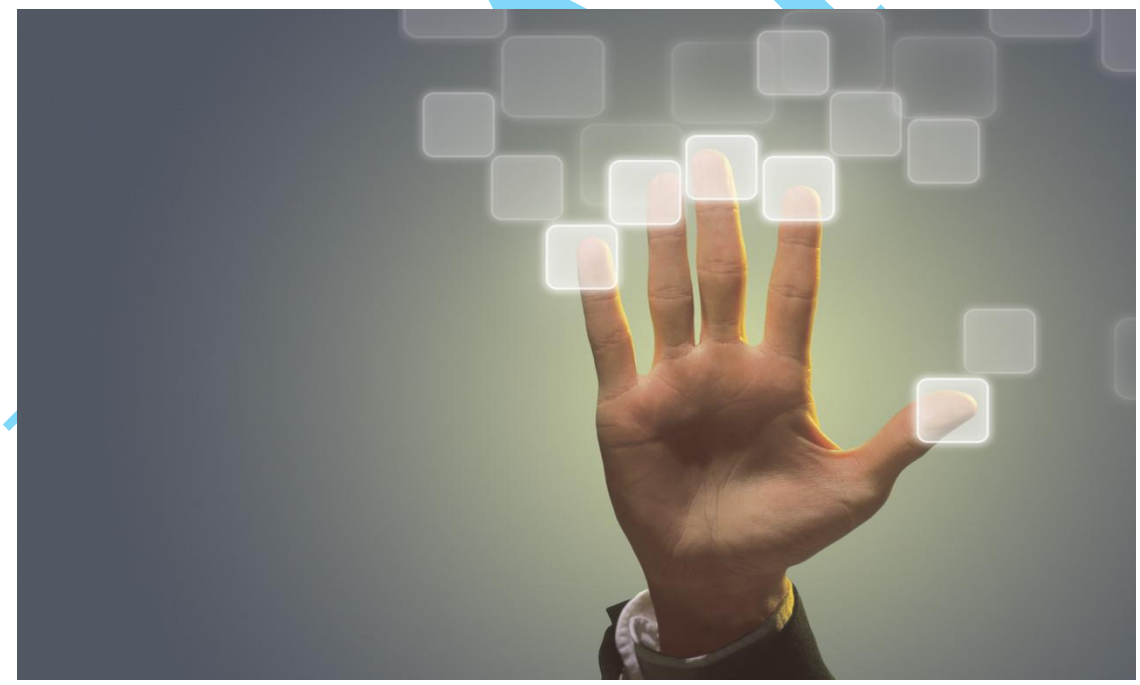
U.S. Department of Housing & Urban Development

PERSONNEL SECURITY

AND

SUITABILITY POLICY



HANDBOOK 755.1

Last revised 5/10/2016

INTRODUCTION

The goal of the Department of Housing and Urban Development's (HUD), Personnel Security and Suitability Program (PSSP), is to ensure the Department will employ and retain only those persons who meet all federal requirements for suitability and whose employment or conduct will not jeopardize the efficiency of the civil service or pose a risk to national security pursuant to 5 CFR §§ 731 and 1400.

Federal requirements for suitability and security aim to promote the efficiency of the civil service and protect national security interests. The Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) mandates security and suitability reform and reporting requirements. Consistent with IRTPA, Executive Order (E.O.) 13467 founded a Suitability and Security Clearance Performance Accountability Council (PAC and Council are used interchangeably). The three permanent members of PAC are the Deputy Director for Management, Office of Management and Budget (OMB), who serves as the Chair; the Director of the Office of Personnel Management, who serves as the Suitability Executive Agent; and, the Director of the Office of the Director of National Intelligence (ODNI), who serves as the Security Executive Agent. The Council was established to lead reform efforts designed to improve the quality, efficiency, and timeliness of the Federal Government's personnel security and suitability processes, which are being implemented in phases through calendar year 2017.

The Office of the Human Capital Officer (OCHCO) is responsible for the administration of this policy. Approval to deviate from this policy must be obtained from HUD's Chief Human Capital Officer.

CHAPTER 1. GENERAL

1-1 Purpose

This handbook includes policies, procedures, and *minimum* standards for the administration of HUD's personnel security and suitability, and credentialing determination programs. This handbook may require modification as implementation of new reform processes emerge through calendar year 2017.

1-2 Authorities/References

1. E.O. 13526, "Classified National Security Information," December 29, 2009
2. E.O.13488, "Granting Reciprocity on Excepted Service and Federal Contractor Employee Fitness and Reinvestigating Individuals in Positions of Public Trust," January 16, 2009
3. E.O. 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
4. E.O. 12968, "Access To Classified Information," August 2, 1995 as amended
5. E.O. 10450, "Security Requirements for Government Employment," April 27, 1953, as amended
6. E.O. 10577, "Amending the Civil Service Rules and Authorizing a New Appointment System for the Competitive Service," 19 FR 7521, 9315, 3 CFR, 1954-1958 Comp., p. 218. Amended by: EO 10675, August 21, 1956; EO 10745, December 12, 1957; EO 10869, March 9, 1960; EO 12107, December 26, 1978
7. 5 CFR §731, Suitability
8. 5 CFR §1400, Designation of National Security Positions
9. 5 CFR §736, Personnel Investigations
10. 5 CFR §752, Adverse Actions
11. Homeland Security Presidential Directive 12 (HSPD-12): "Policy for a Common Identification Standard for Federal Employees and Contractors," August 27, 2004
12. OPM Memorandum: *Final Credentialing Standards for Issuing Personal Identity Verification Cards Under HSPD-12*, July 31, 2008
13. *Suitability and Security Processes Review: Report To The President, February 2014*,Whitehouse.gov, found at: *https://www.whitehouse.gov/sites/default/files/omb/reports/suitability-and-security-process-review-report.pdf*
14. Performance Accountability Council (PAC), "*Security and Suitability Process Reform: Strategic Framework*," February 2010, found at: http://www.nationalsecuritylaw.org/files/received/OMB/Security_and_Suitability_Process_Reform-Strategic_Framework.pdf
15. *Implementation of Federal Investigative Standards for Tier 1 and Tier 2*, FIN 15-03, OPM, November 4, 2014, found at: http://www.opm.gov/investigations/background-investigations/federal-investigations-notices/2015/fin-15-03.pdf
16. *Background Investigations*, OPM, (April 24, 2015), found at: http://www.opm.gov/investigations/background-investigations/

17. *Security and Suitability End-to-End Hiring Roadmap: Elements and Tasks*, OPM (April 24, 2015), found at: http://www.opm.gov/policy-data-oversight/human-capital-management/hiring-reform/securitysuitabilityelements.pdf
18. Cross Agency Priority Goal Quarterly Progress Update: *Insider Threat and Security Clearance Reform*, FY2015 Quarter 1, FAS, (May 11, 2015) found at: http://www.fas.org/sgp/othergov/omb/insider-2015-01.pdf

1-3 Definitions

1. **Agency -** An Executive agency as defined in 5 U.S.C. 105 is an Executive department, a Government corporation, or an independent establishment.
2. **Adjudication –** The evaluation of pertinent data in a background investigation, as well as other available information that is relevant and reliable, to determine whether a covered individual is: (i) suitable for Federal Government employment; (ii) eligible for logical and physical access; (iii) eligible for access to classified information; (iv) eligible to hold a sensitive positions; or (v) fit to perform work for, or on behalf of the Government as a contractor employee (as defined in E.O. 13467).
3. **Applicant** – A person who is being considered or has been considered for employment.
4. **Appointee** – A person who has entered on duty and is in the first year of a subject-to-investigation appointment (as defined in 5 CFR §731.104).
5. **Background Investigations** – Are used as the basis for making security clearance, suitability, or fitness determinations.
6. **Central Verification System (CVS)** – Contains information on background investigations, credentialing determinations, suitability determinations, and security clearances.
7. **Contractor Employee (Contractors)** – An individual who performs work for or on behalf of any agency, under a contract and who, in order to perform the work specified under the contract, will require access to space, information, information technology systems, staff, or other assets of the Federal Government. Such contracts, include, but are not limited to: (i) personal services contracts; (ii) contracts between any non-Federal entity and any agency; and (iii) sub-contracts between any non-Federal entity and another non-Federal entity to perform work related to the primary contract with the agency. (as defined in E.O. 13488).
8. **Core Duty** - A continuing responsibility that is of particular importance to the relevant *covered position* or the achievement of an agency's mission.
9. **Covered Position** – A position in the competitive service; a position in the excepted service where the incumbent can be noncompetitively converted to the competitive service; and, a career appointment to a position in the Senior Executive Service.
10. **Damage** – Harm to the national defense or foreign relations of the United States from the unauthorized disclosure of information, taking into consideration such aspects of the information as the sensitivity, value, utility, and provenance of that information.
11. **Days** – Calendar days unless otherwise specified.
12. **Employee –** An individual who has completed the first year of a subject-to-investigation appointment.
13. **Exceptionally Grave Damage –** The capacity to cause extremely serious harm.

14. **Federal Employment -** Includes the following range of services performed for the Federal Government: (i) All employment in the competitive or excepted service or the Senior Executive Service in the Executive Branch; (ii) appointments, salaried or unsalaried, to Federal Advisory Committees or to membership agencies; (iii) cooperative work assignments in which the individual has access to Federal materials such as examination booklets, or performs service for, or under supervision of, a Federal agency while being paid by another organization such as a State or local government; (iv) volunteer arrangements in which the individual performs service for, or under the supervision of, a Federal agency; and (v) volunteer or other arrangements in which the individual represents the United States Government or any agency thereof.
15. **Fitness –** The level of character and conduct determined necessary for an individual to perform work for or on behalf of a Federal agency as an employee in the excepted service (other than a position subject to suitability) or as a contractor employee.
16. **Human Resources (HR) –** HUD's Recruitment and Staffing Division (RSD).
17. **Inestimable Damage –** The capacity to cause harm too severe to be computed or measured.
18. **Material** - Means, in reference to a statement, one that is capable of influencing, affects, or has a natural tendency to affect, an official decision even if OPM or an agency does not rely upon it.
19. **National Security Position** – As defined in 5 CFR §1400.102, Includes any position in a department or agency, the occupant of which could bring about, by virtue of the nature of the position, a material adverse effect on the national security. Such positions include those requiring eligibility for access to classified information. Other such positions include, but are not limited to, those whose duties include:
    a. Protecting the nation, its citizens and residents from acts of terrorism, espionage, or foreign aggression, including those positions where the occupant's duties involve protecting the nation's borders, ports, critical infrastructure or key resources, and where the occupant's neglect, action, or inaction could bring about a material adverse effect on the national security;
    b. Developing plans or policies related to national defense or military operations;
    c. Planning or conducting intelligence or counterintelligence activities, counterterrorism activities and related activities concerned with the preservation of the military strength of the United States;
    d. Protecting or controlling access to facilities or information systems where the occupant's neglect, action, or inaction could bring about a material adverse effect on the national security;
    e. Controlling, maintaining custody, safeguarding, or disposing of hazardous materials, arms, ammunition or explosives, where the occupant's neglect, action, or inaction could bring about a material adverse effect on the national security;
    f. Exercising investigative or adjudicative duties related to national security, suitability, fitness or identity credentialing, where the occupant's neglect, action, or inaction could bring about a material adverse effect on the national security;

g. Exercising duties related to criminal justice, public safety or law enforcement, where the occupant's neglect, action, or inaction could bring about a material adverse effect on the national security; or
h. Conducting investigations or audits related to the functions described in paragraphs (a)(4)(ii)(B) through (G) of this section, where the occupant's neglect, action, or inaction could bring about a material adverse effect on the national security.

20. **Need for Access** – A determination that an employee requires access to a particular level of classified information in order to perform or assist in a lawful and authorized governmental function.
21. **Need-to-Know -** A determination within the Executive Branch in accordance with directives issued pursuant to E.O.13526 that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function.
22. **Personnel investigation** – An investigation conducted by written or telephone inquiries or through personal contacts to determine the suitability, eligibility, or qualifications of individuals for Federal employment, for work on Federal contracts, or for access to classified information or restricted areas.
23. **Position Designation Automated Tool (PDT) –** Developed by OPM for use by agencies to appropriately designate the risk and sensitivity levels of all Federal competitive positions and any position that can be converted to competitive.
24. **Public Trust Positions** – Positions at the high or moderate risk levels are designated as "Public Trust" positions. Such positions may involve policymaking, major program responsibility, public safety and health, law enforcement duties, fiduciary responsibilities, or other duties demanding a significant degree of public trust; and, positions involving access to—or operation or control of financial records, with a significant risk for causing damage or realizing personal gain. These positions may or may not have access to classified materials.
25. **Risk Designation** – Agency heads (or designee) must designate every *covered position* within the agency at a high, moderate, or low risk as determined by the position's potential for adverse impact to the efficiency or integrity of the civil service. OPM will provide an example of a risk designation system for agency use in an OPM issuance as described in 5 CFR §731.102(c).
26. **Security Investigation -** An investigation required for eligibility to hold a sensitive national security position or access to classified information by military, civilian, or government-contractor personnel performing work for, or on behalf of, the government.
27. **Sensitivity Designation –** All positions subject to investigation under suitability also receive a sensitivity designation of Special-Sensitive, Critical-Sensitive, or Noncritical-Sensitive, when appropriate. This designation is complementary to the risk designation, and may have an effect on the position's investigative requirement.
28. **Sponsor –** A sponsor acts on behalf of the Department to request credentials for HUD applicants (employees, contractors, or affiliates). A sponsor may be a federal agency supervisor or other authoritative official, contracting officer or contracting officer's representative.

29. **Suitability –** An investigation of a character and conduct on persons in positions in the competitive service, excepted service (that can be noncompetitively converted into the competitive service) and career appointments to the Senior Executive Service (SES).
30. **Suitability Action** – An outcome (e.g., cancellation of eligibility, removal, cancellation of reinstatement eligibility, debarment, etc.), as specified in 5 CFR § 731, that is taken against an applicant or an appointee by OPM or an agency with delegated authority under the procedures in subparts C and D of this part.
31. **Suitability Determination –** A decision by OPM or an agency with delegated authority that a person is suitable or is not suitable for employment in *covered positions* (i.e., positions in competitive service, excepted service where the incumbent can be noncompetitively converted to the competitive service and career appointments to positions in the Senior Executive Service).
32. **Tier 1 Investigation –** Is for Suitability Investigations. Tier 1 replaces the National Agency Check with Inquiries (NACI) investigation and is used for positions designated as low-risk, non-sensitive, and credentialing. It is also the minimum level of investigation for a final credentialing determination for physical and logical (computer) access. Tier 1 investigations are requested using the Standard Form (SF) SF-85 as described in Federal Investigative Notice (FIN) 15-03 (November 4, 2014).
33. **Tier 2 Investigation –** Is for Suitability Investigations. Tier 2 replaces the Moderate Risk Background Investigation (MBI). This is the investigation for non-sensitive positions designated as moderate risk public trust positions. Tier 2 investigations are requested using the SF-85P (as described in FIN 15-03 (November 4, 2014)).
34. **Tier 3 Investigation –** Will be for National Security Investigations of Non-Critical Sensitive, L, Confidential and Secret Information using the SF-86.
35. **Tier 4 Investigation –** Will be for Suitability and HSPD-12 investigations of High Risk, Public Trust positions using the SF-85P.
36. **Tier 5 Investigation** – Will be for National Security Investigations of Top Secret, Sensitive Compartmented Information, Critical Sensitive, and Special Sensitive positions using the SF-86.
37. **Violation –** Refers to: (1) any knowing, willful, or negligent action that could reasonably be expected to result in an unauthorized disclosure of classified information; (2) any knowing, willful, or negligent action to classify or continue the classification of information contrary to the requirements of this order or its implementing directives; or (3) any knowing, willful, or negligent action to create or continue a special access program contrary to the requirements of this order (E.O. 13526: Classified National Security Information, December 29, 2009).

1-4 Roles and Responsibilities

Chief Human Capital Officer

The Chief Human Capital Officer (CHCO) has been delegated the authority to make security and suitability determinations in accordance with applicable statutes, executive orders, and regulations. The CHCO is specifically responsible for following Executive Agent security and suitability guidance in:

1. Implementing reform procedures and incorporating IT capabilities requirements to the extent practical as appropriate to satisfy reform goals.
2. Reporting on performance progress as required by the Executive Agents and the Deputy Director of Management and Budget.
3. Following Executive Agent security and suitability guidance for:
    a. Implementing reform procedures and incorporating IT capabilities requirements to the extent practical as appropriate to satisfy reform goals;
    b. Reporting on performance progress as required by the Executive Agents and the Deputy Director of Management and Budget;
    c. Cooperating in oversight and audit efforts; and
    d. Planning and resourcing to satisfy reform performance requirements.

Human Capital Services (HCS) Director

The HCS Director is responsible for:

1. Implementing personnel security and suitability policies.
2. Making suitability determinations and taking suitability actions, including limited, agency-specific debarments under 5 CFR §731.103(a)).
3. Cooperating in oversight and audit efforts.
4. Planning and resourcing to satisfy reform performance requirements.
5. Ensuring the appropriate risk level is designated for *covered positions* at HUD.
6. Ensuring the request of the required investigation corresponds to position the designated risk level.
7. Implementing reform policies, processes, and procedures to satisfy personnel security and suitability goals.

Director of the Personnel Security Division (PSD) is HUD's Security Officer and manages the PSD and PIV Branch.

The PSD Director will:

1. Manage HUD's Personnel Security and Suitability Program (PSSP) in accordance with applicable laws and regulations.
2. Develop and/or assist in the development of departmental security, suitability, and personal identification verification policies.
3. Evaluate and report on the effectiveness of the PSSP to HUD senior officials, OPM, and the Executive Agencies for Suitability and Security, Office of Personnel Management and the Office of the Director for National Intelligence, respectively.

4. Obtain periodic internal security reports from HUD organizational components and prepare reports for senior management.
5. Provide planning, support, and advice for HUD senior officials and offices.
6. Establish PSD/Personal Identification Verification (PIV) training requirements compliant with applicable laws and regulations.
7. Establish and serve as Chairperson of a Personnel Security and Suitability working group, consisting of HR, OGC, and ELRD as applicable, to review internal suitability and/or security incidents/indicators and discuss potential actions to be taken.

Personnel Security Division (PSD)

The Personnel Security Specialist will:

1. Coordinate with human resources, human resources services provider, Administrative Officer, Contracting Officer Representatives, General Technical Representative, General Technical Manager or others to establish acceptable position risk/sensitivity levels via the OPM Position Designation Tool.
2. Sponsor the applicant by entering their sponsorship information into USAccess for Personal Identity Verification (PIV) purposes.
3. Determine if applicant already has a favorably adjudicated background investigation via OPM for employees or through prior agency HR or Security offices for HUD contractors.
4. Determine the level of clearance needed and the appropriate level of investigation for national security positions.
5. Set-up Applicant for a HUD accepted background investigation process, via OPM's e-QIP system, and/or review the Applicant's SF-85, Questionnaire for Non-Sensitive Positions; or SF 85P, Questionnaire for Public Trust Positions; or SF-86, Questionnaire for National Security Positions, and OF-306, Declaration for Federal Employment.
6. Receives and reviews the Security Package from the HR Specialist. Package is needed within 10-days of applicant's certification in e-QIP (when applicable). Security Package and consists of:

    a. PIV (Personal Identity Verification) and Pre-Security Form
    b. HUD Management Survey
    c. Position Designation (with copy of OPM Position Designation Tool results)
    d. Resume
    e. Declaration for Federal Employment (OF-306)
    f. Fair Credit Release (if applicable)
    g. HUD Rules of Behavior
    h. FBI Fingerprint Acknowledgement Form

7. Review the candidate's Declaration for Federal Employment (required for new employees), Optional Form (OF) 306. Look for issues that might be considered a basis for finding an individual unsuitable for Federal employment.
8. Initiate "The Initiate Investigation at the Appropriate Level for the Position to be Filled".
9. Review background investigation and FBI fingerprint results.
10. Apply the OPM referral standards and meet adjudication referral requirements when potential disqualifying information is identified, such as, material intentional falsification, diploma mill, etc.
11. Respond to applicant inquiries regarding an unfavorable entry on duty determination based on preliminary checks and/or the background investigation.

Personnel Identification Verification (PIV) Branch

The PIV Credentialing Specialist will:

1. Obtain fingerprints from selected candidate.
2. Recover revoked or suspended credentials and send to PSD.
3. Initiate renewals, reprints, or reissuances of PIV cards.
4. Change the status of a credential due to a security related situation.
5. Collect, destroy, and mark credentials as destroyed in USAccess.
6. Securely send credentials to the Issuer/Activator at another Activation Station when a credential is shipped to a location where an Applicant does not work.
7. Investigate and resolve enrollment issues such as flagged I-9 documents and possible duplicate records.

Supervisor/Manager

The Supervisor will:

1. Validate the need for the new position in accordance with consistent with, staffing and recruitment plans.
2. Confirm the accuracy of the position description, prior to submitting a recruitment request to HR. If the position description does not accurately describe the position, modify the position description (working with HR) to ensure it correctly describes the position.
3. Work with HR and PSD to properly designate the position for Risk or Sensitivity, in accordance with OPM requirements, using the OPM Position Designation Tool. Such designation is the basis for consistent and proper investigation and reinvestigation, based on the position.

Human Resources and/or HR Service Provider

The HR Specialist will:

1. Work with the supervisor/manager to ensure the position description accurately describes the position and the designation of risk or sensitivity associated with the position is appropriate
2. Identify the core duties in the position description to determine if any are *public trust* duties and whether any could impact the efficiency or integrity of the service. Identify the nature of the position to determine clearance requirements or otherwise impact national security. **Note**: The risk and sensitivity levels of positions are typically determined during the classification process, but must be validated. Use of the OPM Position Designation Tool is required for consistent determinations.
3. Coordinate with supervisors and PSD to establish acceptable position risk/sensitivity levels.
4. Ensure the manager completes or validates the Management Survey and submits it at the time of the initiation of the Power Recruit.
5. Receive applicant selection notification.
6. Issue the employment offer to the selected candidate:
    - The offer may be conditional based on subsequent determinations that the person is suitable for Federal employment and that the person's appointment is clearly consistent with the interests of the national security at the sensitivity level designated.
    - Offer may be conditional based upon a subsequent finding that the person is eligible to have access to classified information or hold a security clearance at the required level.
7. Electronically submit the Onboarding Security Packet to the PSD at PSDFederalInbox@HUD.gov.
8. Review and submit the following documents (completed by selected candidate) to PSD within 48 hours of receipt:
    - Declaration for Federal Employment, OF-306
    - Fair Credit Release
    - HUD Rules of Behavior
    - Resume
    - FBI Fingerprint Acknowledgement Form Personal Identity Verification (PIV) and Pre-Security Form
    - HUD Management Survey
    - Position Sensitivity Designation Document
9. Extend Official/Final offer of employment to selectee if PSD returns a favorable pre-employment security approval decision.

Contracting Officer's Representative (COR), also referred to as General Technical Manager (GTM)/General Technical Representative (GTR)

The COR will:

1. Notify the HUD contractor to complete a security package, which consists of:
   a. PIV (Person Identity Verification) and Pre-Security Form
   b. Declaration for Federal Employment (OF-306)
   c. Fair Credit Release
   d. HUD Rules of Behavior
   e. FBI Fingerprint Acknowledgement Form
   f. HUD Management Survey
   g. Position Designation (with copy of OPM Position Designation Results)
2. Sponsor the applicant by entering their sponsorship information into USAccess, for PIV purposes.
3. Initiate the HUD contractor into e-QIP and advises the HUD contractor to complete the questionnaire within 7 days.
4. Electronically submit the entire HUD Contractor Security Package to the PSD at PSDContractorIn-Box@hud.gov after the HUD contractor has been fingerprinted, completed the on-line security questionnaire, and signed all forms.
5. Assure e-QIP signature pages are submitted to PSD within 10-days of applicant's certification.
6. Ensure HUD contractors do not begin any work for HUD until a Security Approval Notice (SAN) from PSD has been issued.

Employee and Labor Relations Division (ELRD)

The ELRD will:

1. Take suitability actions permitted under HUD's authority, and under the authorities of 5 CFR 731 and 5 CFR 752 (Suitability and Adverse Action, respectively).
2. Identify the employee's due process rights when found unsuitable by PSD.
3. Take adverse actions resulting from investigation of persons or post arrests after a favorable suitability decision is made by PSD.
4. Carry out OPM debarment actions.
5. Collaborate with management to make discipline/adverse action determinations on post-employment arrest issues.

Director of the Office of Personnel Management (OPM)

E.O. 13467 designated the Director of the Office of Personnel Management as the Suitability Executive Agent. As the Suitability Executive Agent, the Director of OPM has the following roles and responsibilities:

1. Developing and implementing uniform and consistent policies and procedures to ensure the effective, efficient, and timely completion of investigation and adjudications relating to determinations of suitability and eligibility for logical and physical access.
2. In addition, Sections 2.4 and 3 of E.O. 13467 reserved and reaffirmed the OPM Director's existing authorities. These include:
3. Executing, administering, and enforcing civil service laws, rules, and regulations, and regulating and enforcing statutes and executive orders conferring responsibilities on OPM, including those concerning suitability and security (5 U.S.C. §§ 1103, 1104; E.O. 10577);
4. Conducting security, suitability, and credentialing investigations for the competitive service (and for the excepted service upon request); conducting investigations for the Department of Defense (including security clearance investigations for Defense contractors and the Armed Forces); and conducting reimbursable investigations (E.O. 10450; E.O. 10577; 5 U.S.C. §§ 1304, 9101);
5. Maintaining an index of security investigations; approving reemployment of persons who have been summarily removed on national security grounds; conducting an ongoing review of agencies' personnel security programs; and reporting compliance to the National Security Council (E.O. 10450);
6. Establishing suitability standards, conducting suitability adjudications, and taking suitability actions for the competitive service (E.O. 10577); and
7. Conducting oversight of agencies' compliance with the civil service rules, and of their performance of delegated investigative and adjudicative authorities (5 U.S.C. §§ 1104, 1303; E.O. 10577).
8. Further, under a subsequent order, E.O. 13488, OPM prescribes fitness reciprocity requirements for contract and excepted service employment, reinvestigation requirements for contract and excepted service employment, and reinvestigation requirements for public trust positions.

Director of National Intelligence (ODNI)

E.O. 13467 designated the Director of the Office of National Intelligence as the Security Executive Agent. The Security Executive Agent is one of the two permanent members of the PAC. As the Security Executive Agent, the Director of the ODNI:

1. Shall direct the oversight of investigations and determinations of eligibility for access to classified information or eligibility to hold a sensitive position made by any agency;
2. Shall be responsible for developing uniform and consistent policies and procedures to ensure the effective, efficient, and timely completion of investigations and adjudications relating to determinations of eligibility for access to classified information or eligibility to hold a sensitive position;
3. May issue guidelines and instructions to the heads of agencies to ensure appropriate uniformity, centralization, efficiency, effectiveness, and timeliness in processes relating to determinations by agencies of eligibility for access to classified information or eligibility to hold a sensitive position;
4. Shall serve as the final authority to designate an agency or agencies to conduct investigations of persons who are proposed for access to classified information to ascertain whether such persons satisfy the criteria for obtaining and retaining access to classified information or eligibility to hold a sensitive position;
5. Shall serve as the final authority to designate an agency or agencies to determine eligibility for access to classified information in accordance with Executive Order 12968 of August 2, 1995;
6. Shall ensure reciprocal recognition of eligibility for access to classified information among the agencies, including acting as the final authority to arbitrate and resolve disputes among the agencies involving the reciprocity of investigations and determinations of eligibility for access to classified information or eligibility to hold a sensitive position; and
7. May assign, in whole or in part, to the head of any agency (solely or jointly) any of the functions detailed the items above, with the agency's exercise of such assigned functions to be subject to the Security Executive Agent's oversight and with such terms and conditions (including approval by the Security Executive Agent) as the Security Executive Agent determines appropriate.

CHAPTER 2. EMPLOYEE SUITABILITY/CONTRACTOR FITNESS OVERVIEW

This chapter outlines suitability/fitness requirements and procedures with regard to Federal employees in *covered positions* and for individuals who perform work on behalf of the Federal government, respectively. While *suitability* and *fitness* determinations both apply the same standards, each term refers to a distinct group of individuals.

A *suitability determination* is a decision an agency with delegated authority from OPM, on whether a person is suitable or is not suitable for employment in *covered positions* in the Federal Government or a specific Federal agency (as defined in 5 CFR §731). Covered positions include competitive service applicants and appointees; excepted-service positions (e.g., Veteran's Readjustment Act (VRA), whereby the incumbent can be noncompetitively converted to the competitive service; and career appointments to entry-level positions in the Senior Executive Service. Suitability determinations are made by assessing a person's identifiable character traits and past conduct, sufficient to determine whether employment or continued employment in the Federal government would protect the integrity and promote the efficiency of the service.

Conversely, the term *fitness determination* refers to contractor employees and individuals in the excepted service (excluding those positions subject to 5 CFR §731), who are ineligible to convert noncompetitively (5 CFR §302). Akin to suitability, a *fitness* determination is an assessment of character and conduct in deciding whether an individual is fit to perform work for, or on behalf of the government or Federal agency. HUD will adhere to suitability criteria in making fitness determinations. The same investigative and adjudicative standards apply to both Federal employees and HUD contractors.

2-1 Position Designation Requirements

Proper position designation is based on a combined assessment of risk, sensitivity, and if applicable, national security requirements. The resulting designation determines the type of investigation required, how an individual is vetted for a position, and whether a reinvestigation or continuous evaluation is required. **Note:** Risk and sensitivity designations are assigned to positions and not the individuals who occupy those positions.

Applicable positions are assigned two distinct designations. One uses the position description and other supplemental information obtained from management and the security office to assess whether the position has public trust duties that impact the efficiency or integrity of the service. The other assesses the nature of the position to determine clearance requirements or impact to national security.

OPM provides a Position Designation System and Automated Tool to simplify and bring consistency to the position designation process. This tool is available on the OPM website at http://www.opm.gov/investigate. Its use is required for all covered positions, as defined above, and strongly recommended to ensure proper investigation requests for all other positions (contractors, SES, etc.) in the agency.

The first designation is based on the level of risk commensurate with any public trust duties of the position. The three levels of risk are (1) High Risk, (2) Moderate Risk, and (3) Low Risk. Public trust positions are those that an agency head (or delegated authority), designate at the moderate or high-risk level, based on the position's potential for adverse impact on the efficiency or integrity of the service. Positions that do not include public trust duties are designated at the low risk level.

The second designation is the level of sensitivity (noncritical-sensitive, critical-sensitive, and special-sensitive), which is based on the degree of potential damage to the national security, and/or the need for access to classified national security information.

2-2 Investigative Requirements

Minimum investigative requirements for *covered positions* are set forth by OPM and are based on the position's risk and/or national security sensitivity designations as determined by OPM's Position Designation Automated Tool (PDT).

1. All individuals appointed to *covered positions* must undergo a background investigation by OPM or by an agency conducting investigations under delegated authority from OPM (as required in 5 CFR §731). Investigations should be initiated before appointment, but no later than 14 calendar days after placement in the position (5 CFR §731.106(c)).
2. Basic suitability screening is required for all *covered positions*.
3. All positions subject to investigation under (5 CFR §731) must also receive a sensitivity designation of Special-Sensitive, Critical-Sensitive, or Noncritical-Sensitive, when appropriate. The sensitivity designation is complementary to the risk designation, and might affect the position's investigative requirements.
4. HUD personnel who are responsible for position designation are required to use the PDT to determine the proper level of investigation and screening required of *covered positions*.
5. The selection of the appropriate type of investigation to conduct must be based on the designation (i.e., risk and sensitivity) requiring the highest level of screening.
6. If suitability issues develop prior to the required investigation, OPM or the agency may conduct an investigation sufficient to resolve the issues and support a suitability determination or action, when warranted. If the person is appointed, the minimum level of investigation must be conducted as required by 5 CFR §731.106(c) (1).
7. An employee or appointee is not required to undergo a new investigation if he or she has undergone an appropriate level investigation, **except** when the risk level changes to a higher level, due to promotion, demotion, or reassignment. Any upgrade in the investigation required for the new risk level should be initiated within 14 calendar days after the promotion, demotion, reassignment or new designation of risk level is final.

8. Reemployed persons must complete a new Declaration for Federal Employment, OF-306, and new or updated investigative questionnaires (if the public trust or sensitivity level of the new position is the same as their previous one). If the reemployed individual divulges suitability issues on the new OF-306 or investigative questionnaire, basic suitability screening will be required. If favorable, a new investigation and adjudication may still be required.

9. Exceptions to the investigative requirements: intermittent, seasonal, per diem, or temporary positions (having less than 180 days per year, aggregately, in either a single continuous appointment or series of appointments); positions filled by aliens employed outside the United States; or other positions that OPM deems appropriate, based on a written request from an agency head where the position is located.

2-3 Reciprocity of Fitness and Suitability Determinations of Federal Employees and Contractor Employees

Both 5 CFR §§ 731.104 and 731.202 require reciprocal acceptance of prior suitability investigations and adjudications. **Note:** The granting of reciprocity does not replace HUD's Onboarding process. Agencies making fitness determinations shall grant reciprocal recognition to a prior favorable fitness or suitability determination when the:

1. Gaining agency uses criteria for making fitness determinations equivalent to suitability standards established by the Office of Personnel Management;

2. Prior favorable fitness or suitability determination was based on criteria equivalent to suitability standards established by the Office of Personnel Management; and after validating need through the appropriate systems and the review of a complete security package to include the security questionnaire, an investigation conducted with a favorable adjudication within the past five years and no more than a two year break service. Only when an investigation at the same or higher level was favorably adjudicated for another federal agency on a federal/contract employee as the one required, is the investigation sufficient to meet the investigation requirements.

3. Any break in service can result in the need for a new investigation. However, 5 CFR §731 allows appointment to a covered position where there has been a break in service of less than 24 months, and the service immediately preceding the break was in a covered position, an excepted service position, or contract employee position described in paragraphs (a)(1) to (a)(4) of section 731.104. If that investigation is unavailable or not made available within a reasonable amount of time, a new appropriate investigation and pre-employment security approval must be initiated.

Exceptions to Reciprocal Recognition

A gaining agency is not required to grant reciprocal recognition to a prior favorable fitness or suitability determination when:

1. The new position requires a higher level of investigation than previously conducted for that individual;

2. An agency obtains new information that calls into question the individual's fitness based on character or conduct; or
3. The individual's investigative record shows conduct that is incompatible with the core duties of the new position.

2-4 Criteria for Making Suitability/Fitness Determinations

Suitability determinations for Federal employment are required to be made based on the presence or absence of one or more of the below specific factors (charges), as prescribed in 5 CFR §731.202. Only these eight (8) specific factors are to be considered a basis for finding a person unsuitable and taking a suitability action:

1. Misconduct or negligence in employment;
2. Criminal or dishonest conduct;
3. Material, intentional false statement, or deception or fraud in examination or appointment (OPM retains the right to adjudicate this factor);
4. Refusal to furnish testimony as required by 5 CFR §5.4 (Only OPM can cite this factor);
5. Alcohol abuse, without evidence of substantial rehabilitation, of a nature and duration that suggests that the applicant or appointee would be prevented from performing the duties of the position in question, or would constitute a direct threat to the property or safety of the applicant or appointee or other;*
6. Illegal use of narcotics, drugs, or other controlled substances without evidence of substantial rehabilitation;*

   **Neither factor applies if there is clear evidence of substantial rehabilitation (measurable efforts and noticeable results*)

7. Knowing and willful engagement in acts or activities designed to overthrow the U.S. Government by force; and
8. Any statutory or regulatory bar, which prevents the lawful employment of the person, involved in the position in question.

Additional considerations:

The following additional considerations to the extent that HUD or OPM, in its sole discretion, deems any of them pertinent to the individual case:

1. The nature of the position for which the person is applying or in which the person is employed;
2. The nature and seriousness of the conduct;
3. The circumstances surrounding the conduct;

4. The recency of the conduct;
5. The age of the person involved at the time of the conduct;
6. Contributing societal conditions; and
7. The absence or presence of rehabilitation or efforts toward rehabilitation

An agency cannot make a new determination for a person who has already been determined suitable or fit based on character or conduct, unless a new investigation is required under 5 CFR §731.104 or §731.106, or no new investigation is required, but the investigative record on file for the person reveals conduct that is incompatible with the core duties of the relevant covered position.

2-5 Adjudication

The agency is to adjudicate the suitability of all *covered positions* and fitness of contractors for HUD except when there is evidence of material intentional false statement, deception, or fraud in examination or appointment, or evidence of a refusal to furnish testimony, in which OPM retains the authority to adjudicate. Agencies are responsible for identifying admitted and developed issues prior to appointment and may use OPM's "Referral Chart: Information Requirements for Suitability Referrals (see Appendix B)," to determine which issues or combinations of issues warrant referral to the HUD's adjudications office for suitability review and adjudication. The agency adjudication office is responsible for assessing the issues and determining which cases require referral to OPM for debarment consideration.

2-6 Suitability Actions (Excludes Contractor Employees)

A HUD suitability authority or OPM may investigate and take one or more of the following suitability actions against an *applicant* or *appointee* (an individual within the first year of service) of a covered position, who is deemed unsuitable for Federal employment based on the criteria under 5 CFR §731.202, subject to the agency limitations of 5 CFR §731.103(g). OPM retains jurisdiction on *employees* (i.e., individuals having more than one year of continuous federal service).

- Cancellation of eligibility
- Removal
- Cancellation of reinstatement eligibility
- Debarment

1. An agency may not take a *suitability* action against an *employee* (a person who has completed one year of federal service); however, the agency may be able to take an adverse action under 5 CFR §752.

2. Agencies do not need approval from OPM before taking unfavorable suitability actions. However, the Agency is required to report to OPM all unfavorable suitability actions taken under this part within 30 days after they take the action. In addition, all

actions based on an OPM investigation must be reported to OPM as soon as possible and in no event later than 90 days after receipt of the final report of investigation.

3. Agencies must refer to OPM all suitability cases where there is evidence of material, intentional falsification, or deception or fraud in examination or appointment; or refusal to furnish testimony as required by 5 CFR §5.4, for final determinations and to take action. **NOTE**: In cases involving falsification, deception, fraud, or refusal to furnish testimony, agencies can elect to proceed with an action under a different authority—without prior approval by OPM; however, notification of the case to OPM is required.

4. Agencies are required to refer cases to OPM when it appears a Government-wide debarment may be warranted (as described in 5 CFR §731.204).

5. OPM may require that an appointee or an employee be removed on the basis of a material, intentional false statement, deception or fraud in examination or appointment; refusal to furnish testimony as required by 5 CFR §5.4; or a statutory or regulatory bar which prevents the person's lawful employment.

6. OPM may cancel any reinstatement eligibility obtained for a material, intentional false statement, deception, or fraud in examination or appointment.

7. Agencies must give reasonable notice to the applicant or appointee (hereinafter, the "respondent") in writing of the proposed action, the charges against the respondent, and the availability for review, upon request, of the materials relied upon.

    a. The notice must set forth the specific reasons for the proposed action and state that the respondent has the right to answer the notice in writing. The notice must further inform the respondent of the time limit for the answer as well as the address to which such answer must be delivered.
    b. The notice must inform the respondent that a representative of the respondent's choice may represent him or her and that if the respondent wishes to have such a representative, the respondent must designate the representative in writing.
    c. The agency must serve the notice of proposed action to respondent by mail or hand delivery no less than 30 days prior to the effective date of the propose action to the respondent's last known residence or duty station.
    d. If the respondent is employed in a position covered by this part on the date the notice is served, the respondent is entitled to be retained in a pay status during the notice period.
    e. A respondent may answer the charges in writing and furnish documentation and/or affidavits in support of the answer. To be timely, a written answer must be submitted no more than 30 days after the date of the notice of proposed action. If OPM initiates a suitability action, the employing agency may also answer the notice of proposed action. The time limit for filing such an answer

is 30 days from the date of the notice. In reaching a decision, OPM will consider any answer the agency makes.

8. Requests to pass over a preference eligible for reasons based on conduct are handled by OPM's Federal Investigative Services, NACI [National Agency Check with Inquiries] & Agency Referral Adjudications branch.

2-7 Fitness of Contractor Employees

Under no circumstances can an "unfit" determination of a contractor employee (hereinafter called contractor) be appealed. Contractors deemed "unfit" will be notified in writing of an unfavorable determination with regard to his/her ineligibility to render services or otherwise perform under the specified HUD contract. Unfavorable information discovered in HUD's fitness determination will not be disclosed to the contractor's employer. An unfavorable determination by HUD's personnel security specialists in no way implies that the contractor is "unfit" for employment outside of HUD.

2-8 Reinvestigations of Individuals in Positions of Public Trust

All Public Trust positions require the incumbent to undergo reinvestigations at least once, every 5 years.

1. For consistency, OPM requires all Federal agencies to follow the same reinvestigation schedule.
2. A person's employment status will determine the applicable HUD authority and procedures to be followed in any action taken based on the results of the reinvestigation.
3. Conduct that surfaces during a reinvestigation could form the basis for an adverse action under 5 CFR §752. Whether to propose and take an adverse action based on a public trust reinvestigation is a matter within the employing agency's discretion.
4. HUD will use OPM's Position Designation Automated Tool, and will re-designate positions as appropriate, such as when duties of the position change. If position requirements change, an agency should use OPM's Position Designation System to determine any new investigation requirement and subsequent reinvestigation requirements.
5. In order to determine the proper designation of a position, the position description and any other necessary supplemental information (e.g., management and security office input) must be carefully evaluated to assess the nature of the position in terms of its clearance requirements or any other impact on national security as well as its impact on the efficiency or integrity of the service.
6. OPM retains jurisdiction to make final determinations and take actions in all suitability cases where there is evidence that there has been a material, intentional false statement, or deception or fraud in examination or appointment. OPM also

retains jurisdiction over all suitability cases involving a refusal to furnish testimony as required. Nonetheless, conduct that surfaces during a reinvestigation could form the basis for an adverse action under 5 CFR §752. Whether to propose and take an adverse action based on a public trust reinvestigation is a matter within the employing agency's discretion.

7. Issues developed in reinvestigations must be evaluated to determine whether or not the person's continued employment promotes the efficiency of the service; however, agencies have no jurisdiction to take actions on employees (continuous service for more than a year) under 5 CFR §731. Any necessary action, must be taken under other agency authority (e.g., 5 CFR §752).

2-9 Suitability/Fitness Reporting Requirements

Agencies must report to OPM the level or nature, result, and completion date of each background investigation or reinvestigation, each agency decision based on such investigation or reinvestigation and any personnel action taken based on such investigation or reinvestigation, as required under OPM authority (5 CFR §731.206). Agencies must report adjudication outcomes to OPM through paper or electronic Forms 79A, *Report of Agency Adjudicative Action*, as soon as possible, and no later than 90 days after receiving the investigation from OPM (as described in FIN Notice 13-04)

2-10 Appeal to the Merit Systems Protection Board (Excludes Contractor Employees)

According to 5 CFR §731.501, when a delegated authority of HUD or OPM takes a suitability action against a person, that person may appeal the action to the Merit Systems Protection Board (hereinafter "Board").

Decisions by the Merit Systems Protection Board

1. If the Board finds that one or more of the charges brought by OPM or an agency against the person is supported by a preponderance of the evidence, regardless of whether all specifications are sustained, it must affirm the suitability determination. The Board must consider the record as a whole and make a finding on each charge and specification in making its decision.
2. If the Board sustains fewer than all the charges, the Board must remand the case to OPM or the agency to determine whether the suitability action taken is appropriate, based on the sustained charge(s). However, the agency must hold in abeyance a decision on remand, until the person has exhausted all rights to seek review of the Board's decision to include court review.
3. Once review is final, OPM or an agency will determine whether the action taken is appropriate based on the sustained charges and this determination will be final without any further appeal to the Board.
4. *Appeal procedures.* The procedures for filing an appeal with the Board is found in 5 CFR part 1201.

CHAPTER 3. NATIONAL SECURITY OVERVIEW

Any position in the Federal service requiring access to classified information or otherwise impacts the national security, must be assigned a sensitivity designation. Security clearances are granted on a "need-to-know" basis when there is a demonstrated need for access to classified information (E.O. 12968). The designation of National Security positions is outlined in section 3 of E.O. 10450, as amended, and in 5 CFR § 1400. Accordingly, the Secretary for HUD:

1. Shall designate, or cause to be designated, any position within the department or agency the occupant of which could bring about, by virtue of the nature of the position, a material adverse effect on the national security as a sensitive position at one of three sensitivity levels: Special-Sensitive, Critical-Sensitive, or Noncritical-Sensitive.
2. Will minimize the number of employees eligible for access to classified information that the agency determines is required to conduct agency functions.

3-1 Sensitivity Level Designation

To assure that the risk inherent in the hiring and placement decisions are managed properly, it is essential that all positions be designated with correct and consistent sensitivity levels. Positions are to be designated using OPM's Position Sensitivity Designation Tool and guidance. Positions designated as *Non-Sensitive* do not require access to classified information.

1. **Noncritical-Sensitive** – Assigned to positions having the potential to cause *damage* to the national security, up to and including damage at the significant or serious level. Eligibility for access to Confidential and Secret classified national security information.
2. **Critical-Sensitive** – Assigned to positions having the potential to cause exceptionally grave damage to national security. Eligibility for access to Top Secret classified national security information.
3. **Special-Sensitive** – Assigned to positions having the potential to cause inestimable damage to the national security. Eligibility for access to Top Secret classified national security information and Sensitive Compartmented Information (SCI).

3-2 Security Clearance Levels

Information requiring a security clearance may be classified at one of the following three security clearance levels pursuant to E.O. 13526:

- **Top Secret** – Shall be applied to information that the unauthorized disclosure of which reasonably could be expected to cause exceptionally *grave damage* to the national security that the original classification authority is able to identify or describe.

- Reinvestigations are currently conducted every 5 years; however, the Director of National Intelligence, as the Executive Agent for Security is moving toward a continuous evaluation of Top Secret clearance holders, through a series of automated records checks to be adjudicated by the agency granting the clearance.
- To the extent practical, the investigative phase (conducted by OPM) should be achieved within a period of no longer than 80 days for a Top Secret (critical sensitive or special sensitive, Tier 5) investigation, after the date of receipt of the completed application for a security clearance via e-QIP.

- **Secret –** Shall be applied to information that the unauthorized disclosure of which reasonably could be expected to cause *serious damage* to the national security that the original classification authority is able to identify or describe.
  - Reinvestigations, as of October 2015, are to be conducted every 5 years.
  - To the extent practical, the investigative phase (conducted by OPM) should be achieved within a period of no longer than 40 days for a Secret (non-critical Sensitive, Tier 3) investigation, after the date of receipt of the completed application for a security clearance via e-QIP.

- **Confidential** – Applies to the unauthorized disclosure of information, which reasonably could be expected to cause *damage* to the national security that the original classification authority is able to identify or describe.
  - Reinvestigations, as of October 2015, are to be conducted every 5 years.
  - To the extent practical, the investigative phase (conducted by OPM) should be achieved within a period of no longer than 40 days for a Secret (non-critical Sensitive, Tier 3) investigation, after the date of receipt of the completed application for a security clearance via e-QIP. The "Secret" clearance is the lowest level security clearance and allows access to "Confidential" classified information.

3-3 Investigation Requirements

National Security investigations are required for eligibility to hold a *sensitive* national security position or to access classified information by civilian, military, or government contractor personnel who perform work for, or on behalf of the government. Security investigations provide an assessment of an individual's potential likelihood to promote the efficiency and integrity of the Federal service and for determining whether employment or retention in employment is in the interests of national security.

1. All civilian officers or employees of the Federal Government are subject to investigation.
2. Employees may be considered for access to classified information only when such access is required in connection with official duties.

3. Investigative requirements for each sensitivity level are provided in OPM issuances.
4. In general, investigations must be initiated within 14 days of placement in a position. Exceptions under 5 CFR §1400.202 include positions designated as:
    a. Critical-Sensitive – Investigations must be completed preplacement, but may be completed post-placement with approval of a waiver.
    b. Special-Sensitive – Investigations must be completed preplacement.

3-4 Reciprocity for Security Clearances

Reciprocity aims to eliminate duplication when conducting background investigations and adjudications at the equivalent level. However, under no circumstance does reciprocity replace HUD's Pre-employment Security Approval process.

1. An authorized investigative agency or authorized adjudicative agency may not conduct an investigation for purposes of determining whether to grant a security clearance to an individual, where a current investigation or clearance of equal level already exists, or has been granted by another authorized adjudicative agency.
2. Agencies are required to accept a security clearance granted by another Federal agency; this ensures background investigations are only conducted to grant new security clearances.
3. Agencies must record their security clearances in central databases, even when accepting reciprocity.
4. Previous approval must have been granted within the last 24 months and there must have been no break in employment.

Exceptions to Reciprocal Recognition

A gaining agency is not required to grant reciprocal recognition in cases where:

1. Substantial information emerges that employee may not satisfy the standards.
2. Existing security clearance was discretionary—did not meet adjudicative or investigative standards (conditions, deviations, and waivers).
3. Exceptional circumstances exist for special access programs are additional, but not duplicative, procedures are required to protect the national security (e.g., polygraph, non-U.S. immediate family members).
4. Proof of a favorable adjudication and granting of a security clearance cannot be located.

3-5 Adjudication/Appeals

A decision to grant a security clearance should be made after the final suitability determination has been made. The Intelligence Reform and Terrorism Prevention Act (IRTPA) established standards for adjudicative timeliness for National Security reviews, whereby the adjudicative phase should be finalized within a period of no longer than 20 days.

When determining eligibility for access to classified information, adjudicators will use the "Adjudicative Guidelines for Determining Eligibility for Access to Classified Information," (hereinafter called, "Adjudicative Guidelines" or successor guidelines), either to make a favorable decision or to identify disqualifying information and deny or revoke the clearance.

Agency adjudicators will use the information from the investigative report to determine whether to grant or deny a person's eligibility for security clearance by considering guidelines in specific areas that elicit information about: (1) conduct that could raise security concerns; and (2) factors that could dispel those security concerns and permit granting of a clearance. The following adjudicative guidelines apply to persons being considered for initial or continued eligibility for access to classified information to include sensitive compartmented information and special access programs, and are to be used by government departments and agencies in the executive branch, for all final clearance determinations.

Adjudicative Guidelines for Determining Eligibility for Access to Classified Information

(1) Guideline A: Allegiance to the United States.
(2) Guideline B: Foreign influence.
(3) Guideline C: Foreign preference.
(4) Guideline D: Sexual behavior.
(5) Guideline E: Personal conduct.
(6) Guideline F: Financial considerations.
(7) Guideline G: Alcohol consumption.
(8) Guideline H: Drug involvement.
(9) Guideline I: Psychological Conditions.
(10) Guideline J: Criminal conduct.
(11) Guideline K: Handling Protected Information.
(12) Guideline L: Outside activities.
(13) Guideline M: Misuse of Information Technology Systems.

Although adverse information concerning a single criterion may not be sufficient for an unfavorable determination, the individual may be disqualified if available information reflects a recent or recurring pattern of questionable judgment, irresponsibility, or emotionally unstable behavior. Notwithstanding the whole person concept, pursuit of further investigations may be terminated by an appropriate adjudicative agency in the face of reliable, significant, disqualifying, adverse information.

When information of security concern becomes known about an individual who is currently eligible for access to classified information, the adjudicator should consider whether the person:

(1) Voluntarily reported the information;
(2) Was truthful and complete in responding to questions;
(3) Sought assistance and followed professional guidance, where appropriate;
(4) Resolved or appears likely to resolve favorably the security concern;
(5) Has demonstrated positive changes in behavior and employment;
(6) Should have his or her access suspended temporarily pending final adjudication of the information.

If after evaluating information of security concern, the adjudicator decides that the information is not serious enough to warrant a recommendation of denial or revocation of the security clearance, it may be appropriate to recommend approval with a warning that future incidents of a similar nature may result in revocation of access.

- Each case must be judged on its own merits, and final determination remains the responsibility of the specific department or agency. Any doubt as to whether

access to classified information is clearly consistent with national security will be resolved in favor of the national security.

Appeals

Appeal procedures may be found in Appendix C.

3-6 General Restrictions on Access to Classified Information

Pursuant to E.O. 13526, a person may have access to classified information if:

1. A favorable determination of eligibility for access has been made by an agency head or the agency head's designee;
2. The person has signed an approved nondisclosure agreement; and
3. The person has a *need-to-know* the information.

- Persons meeting these standards must receive concurrent training on the proper safeguarding of classified information and on the criminal, civil, and administrative sanctions that may be imposed on an individual who fails to protect classified information from unauthorized disclosure.

3-7 HUD Reporting Requirements

Pursuant to 5 CFR §732.302, to assist OPM in fulfilling its responsibilities under E.O. 10450, the head (or designee) of each department or agency, conducting a security investigation under E.O. 10450 is required to:

a) Notify OPM when the investigation is initiated (Section 9(a) of E.O. 10450).

b) Report to OPM the action taken with respect to individuals investigated pursuant to E.O. 10450 as soon as possible and in no event later than 90 days after receipt of the final report of security investigation (Section 14(c) of E.O. 10450).

3-8 Reinvestigation Requirements

The incumbent of a national security (Sensitive) position requiring eligibility for access to classified national security information is subject to reinvestigation requirements in accordance with E.O. 12968 and 5 CFR §1400. Positions designated as Special-Sensitive, Critical-Sensitive, and Non-Critical Sensitive are subject to investigation for initial placement and at least once for each succeeding 5 years.

The employing agency will use the results of such periodic reinvestigation to determine whether the continued eligibility to occupy a sensitive position is clearly consistent with the interests of the national security (in accordance with 5 CFR §1400).

3-9 Continuous Evaluation

E.O. 13467 amended E.O. 12968 by requiring that "an individual who has been determined to be eligible for, or who currently has access to classified information, shall be subject to continuous evaluation (CE) under standards (including, but not limited to, the frequency of such evaluation) as determined by the Director of National Intelligence." CE is a personnel security investigative process of reviewing the background of an individual who currently has access to classified information or holds a sensitive position using automated records checks of commercial databases, U.S. Government databases, and other information lawfully available to security officials. The results from this process provide personnel security officials with adjudicative information relevant to determine whether an individual continues to meet the eligibility requirements throughout the period of eligibility. CE is conducted more frequently than periodic reinvestigations intended to enhance Federal personnel security programs.

CHAPTER 4. HOMELAND SECURITY PRESIDENTIAL DIRECTIVE (HSPD)-12

The Homeland Security Presidential Directive (HSPD)-12, mandates government-wide standards for issuing secure and reliable forms of identification to persons requiring access to federally controlled facilities and information systems. The credentialing standards stated in this chapter, are taken from the OPM memorandum, "Final Credentialing Standards for Issuing Personal Identity Verification Cards under HSPD-12," dated July 31, 2008. These standards are used to determine initial eligibility for a personal identity verification (PIV) card.

4-1 Policy

1. All HUD employees, contractors, and students are required to complete the HSPD-12 PIV process, via USAccess, BEFORE reporting for ANY type of appointment.
2. HUD will begin the credentialing process as soon as a person accepts a tentative offer of employment.
3. At a minimum, completion and successful adjudication of Tier 1 formerly known as a National Agency Check with Inquiries (NACI) investigation or other investigation as required for Federal employment will be conducted.
4. HUD will not issue a PIV card unless all preliminary checks (e.g., FBI fingerprint check) are reviewed and adjudicated as favorable.
5. All individuals requiring a PIV card must meet credentialing standards prescribed by OPM (see 4-2 and 4-3). The OPM credentialing standards will be the basis for denying or revoking a PIV card.
6. If an individual, who otherwise meets these standards, is found unsuitable for the competitive civil service under 5 CFR part 731; ineligible for access to classified information under E.O.12968; or, disqualified from appointment in the excepted service or from working on a contract; then, the unfavorable decision is a sufficient basis for non-issuance or revocation of a PIV card.
7. The PIV credentialing process does not interfere with HUD's discretion to make suitability or national security (security clearance) determinations either before or after a person has entered on duty.
8. HUD and HUD's HR service provider will verify employment authorization of all new hires using the I-9 form.

4-2 Basic Credentialing Standards

Agencies may not, waive, modify, replace, or add to credentialing standards (E.O. 13467). In all cases, agencies must apply the minimum HSPD-12 credentialing standards. The minimum standards for initial eligibility for a PIV card are listed below. A PIV card will not be issued to a person if:

1. The individual is known to be or reasonably suspected of being a terrorist;
2. The employer is unable to verify the individual's claimed identity;

3. There is a reasonable basis to believe the individual has submitted fraudulent information concerning his or her identity;
4. There is a reasonable basis to believe the individual will attempt to gain unauthorized access to classified documents, information protected by the Privacy Act, information that is proprietary in nature, or other sensitive or protected information;
5. There is a reasonable basis to believe the individual will use an identity credential outside the workplace unlawfully or inappropriately; or
6. There is a reasonable basis to believe the individual will use federally controlled information systems unlawfully, make unauthorized modifications to such systems, corrupt or destroy such systems, or engage in inappropriate uses of such systems.

If an individual, who otherwise meets these standards, is found unsuitable for the competitive civil service, under 5 CFR part 731; ineligible for access to classified information under E.O. 12968; or, disqualified from appointment in the excepted service or from working on a contract; then, the unfavorable decision is a sufficient basis for non-issuance or revocation of a PIV card.

4-3 Supplemental Credentialing Standards

In cases where individuals do not require a suitability determination or a security clearance (e.g., volunteers, intermittent, temporary, seasonal employees, etc.), agencies have the flexibility to apply the following seven supplemental credentialing standards—in addition to the six basic standards above. These supplemental standards are intended to ensure granting of a PIV card to an individual does not create unacceptable risk, when the individual is not subject to an adjudication of suitability for employment in the competitive service under 5 CFR part 731, qualification for employment in the excepted service under 5 CFR part 302 or similar authority, or eligibility for access to classified information under E.O. 12968. These standards may be applied based on the risk associated with the position or work on the contract.

1. There is a reasonable basis to believe, based on the individual's misconduct or negligence in employment, that issuance of a PIV card poses an unacceptable risk;
2. There is a reasonable basis to believe, based on the individual's criminal or dishonest conduct, that issuance of a PIV card poses an unacceptable risk;
3. There is a reasonable basis to believe, based on the individual's material, intentional false statement, deception, or fraud in connection with Federal or contract employment, that issuance of a PIV card poses an unacceptable risk;
4. There is a reasonable basis to believe, based on the nature or duration of the individual's alcohol abuse without evidence of substantial rehabilitation, that issuance of a PIV card poses an unacceptable risk;
5. There is a reasonable basis to believe, based on the nature or duration of the individual's illegal use of narcotics, drugs, or other controlled substances without

evidence of substantial rehabilitation, that issuance of a PIV card poses an unacceptable risk;

6. A statutory or regulatory bar prevents the individual's contract employment; or would prevent Federal employment under circumstances that furnish a reasonable basis to believe that issuance of a PIV card poses an unacceptable risk; or
7. The individual has knowingly and willfully engaged in acts or activities designed to overthrow the U.S. Government by force.

4-4 Credentialing Process

Credentials may be issued using one of the following options:

Option l--Interim credentialing determination followed by a final credentialing determination:

When a department or agency wishes to bring a new employee or contract employee on board pending completion of a background investigation or any applicable suitability and/or national security decision under 5 CFR part 731 and E.O. 12968, respectively, or any decision as to whether an individual is qualified for an excepted service appointment or to work on a contract, the department or agency may first make an interim credentialing determination. The interim credentialing determination must be based on:

a) The person presenting two identity source documents, at least one of which is a valid Federal or State government-issued picture identification, and
b) A National Agency Check (NAC) or an FBI National Criminal History Check (fingerprint check).

Upon completion of a background investigation, and at the time of a determination of suitability for an appointment in the competitive service under 5 CFR part 731, eligibility for access to classified information under E.O. 12968, or qualification for an appointment in the excepted service or to work on a contract, a department or agency should simultaneously make a final credentialing determination.

Option 2-Single and final credentialing determination before employment:

A department or agency may decide to issue a PIV card only after a single and final credentialing determination is made based on a completed active and favorable background investigation, or after any applicable determination of suitability for an appointment in the competitive service under 5 CFR part 731, eligibility for access to classified information under E.O. 12968, or qualification for an appointment in the excepted service or to work on a contract, is made on the same person.

Reconsideration

- No reconsideration is required when the Department denies a PIV card based on the results of a negative suitability determination under 5 CFR part 731 or a decision to deny or revoke a security clearance. In those situations, the reconsideration process does not apply because the person is already entitled to seek review under applicable suitability or national security procedures.
- There is no right to reconsideration in those situations where the Department denies a PIV card based on the results of a determination to disqualify the person from an appointment in the excepted service or from working on a contract.
- There is no further right of review.

Reciprocity of Credentialing Determinations

- HUD will accept PIV card credentialing determinations for persons transferring from another department or agency when the possession of a valid Federal identity credential can be verified by the person's former department or agency and the individual has undergone the required Tier1 (NACI) or other suitability or National Security investigation at the person's former department or agency.

- At HUD's discretion, a person may be ineligible for a PIV card when the former employing department or agency:
  1. determined he or she is unsuitable for employment in the competitive service under 5 CFR part 731,
  2. denied (or revoked) his or her security clearance under E.O. 12968, or
  3. disqualified the individual from an appointment in the excepted service or from working on a Federal contract. Credentialing determinations are maintained by the granting agency in its Identity Management System (IDMS) and the agency also provides the data to the Central Verification System (CVS) for reciprocity purposes. This will allow agencies to certify to each other the HSPD-12 credentialing of employees and HUD contractor personnel.
- If an unfavorable adjudication occurs for reasons other than the established six basic credentialing standards, and the individual is: later determined to be suitable, granted a clearance, qualified for appointment in the excepted service, or qualified to work on a Federal contract, HUD then, should simultaneously make a new credentialing determination.

Credentialing of non-United States Nationals

Departments and agencies are required to apply the above credentialing process and standards to non-U.S. nationals who work as employees or contractor employees for Federal departments or agencies and may include others who require long-term logical or physical access to Federal government facilities whether overseas or in the United States.

However, special considerations apply to non-U.S. nationals (according to OPM's, *Final Credentialing Standards for Issuing Personal Identity Verification Cards under HSPD-12*, memorandum dated July 31, 2008).

At US-Based Locations and in US Territories (Other than American Samoa and Commonwealth of the Northern Mariana Islands (CNMI)/4:

Departments and agencies must verify employment authorization of new Federal employees with the Department of Homeland Security (DHS) in accordance with OMB Memorandum 07-21, *Verifying the Employment Eligibility of Federal Employees.*

For individuals who are non-U.S. nationals in the United States or U.S. territory for 3 years or more a background investigation (i.e., NACI or equivalent) must be initiated after employment authorization is appropriately verified through E-Verify (or immigration status is appropriately verified for those individuals not working for the Federal Government through the USCIS' Systematic Alien Verification for Entitlements (SAVE) system).

For non-U.S. nationals in the U.S. or U.S. territory for less than three years, agencies may delay the background investigation until the individual has been in the U.S. or U.S. territory for three years. In such cases, an alternative facility-access identity credential may be issued at the discretion of the relevant agency official as appropriate based on a risk determination. *Before* an alternative identity credential may be issued, the individual's employment authorization must be verified and an FBI fingerprint based criminal history must be completed. If the agency decides to delay the background investigation, the agency must request an FBI Investigations Files (name check search), a name check against the Terrorist Screening Database, and a USCIS Check against SAVE.

Agencies may also choose to include additional checks as appropriate. Furthermore, agencies may establish a Special Agreement Check (SAC) with OPM, for conducting the FBI fingerprint based criminal history check and other national agency checks on non-U.S. nationals. Please contact the Agency Liaison Group (ALG) with OPM's Federal Investigative Services Division (FISD) at (703) 603-0442.

At Foreign Locations:

Departments and agencies must initiate and ensure the completion of a background investigation *before* applying the credentialing standards. However, the type of background investigation may vary based on standing reciprocity treaties concerning identity assurance and information exchange that exist between the United States and its Allies or agency agreements with the host country. In most cases, OPM will not be able to conduct a NACI, unless the non-U.S. national is or has been residing in the United States for 3-years or more

The background investigation must be consistent with a NACI to the extent possible and include a fingerprint check against the FBI criminal history database, an FBI

Investigations Files (name check search), and a name check against the Terrorist Screening Database. Agencies may also choose to include additional checks as appropriate.

As in the United States, for those non-U.S. nationals where a NACI or equivalent cannot be performed, an alternative facility-access identity credential may be issued at the discretion of the Department of State Chief of Mission Authority, Department of Defense Installation Commander, and/or other agency official as appropriate based on a risk determination.

Whether at a U.S.-based or foreign location, reciprocity between agencies is not mandatory in the case of alternative identity credentials issued to non-U.S. nationals. Agencies may choose to *honor* such credentials from other agencies, but that is at their discretion.

4-5 Separations

All HUD employees leaving Federal service or transferring to another agency, as well as HUD contractor employees must surrender their PIV/building access card and be cleared by the authorized official in the Headquarters (HQ) PIV office using the *Clearance for Separation of Employee,* HUD-58 or HUD-58A form (whichever is appropriate).

The HUD-58 or HUD-58A will be completed using the Separating Employee Clearance (SEC) tool. The tool allows certification of receipt of the PIV, when an employee relinquishes it.

Separation Procedures:

1. Employees (except those identified in items #2 and #3 below), will surrender their PIV card to their program office's AO or appropriate official in the PIV office.
    - When the AO accepts the PIV card, he/she will certify in SEC having received it and forward it to HQ PIV office, for disabling and destruction

2. Employees serving under the following types of appointments will surrender their PIV card to the appropriate personnel in the Executive Resources Office, who will forward it to HQ PIV office:
    - Schedule C
    - Political Appointees
    - Senior Executive Service (SES)/Senior Level (SL)/Scientific or Professional (ST) Intergovernmental Personnel Act Employee (IPA)

3. Contractors will surrender their PIV card to the Contracting Officer's Representative (COR) also called General Technical Manager (GTM), General Technical Representative (GTR) immediately upon the termination of the HUD

contract. The Office of the Chief Procurement Officer inserts the following clause into every contract solicitation: "...the COR shall be responsible for all PIV cards issued to contract employees and shall immediately notify the GTR if any PIV card(s) cannot be accounted for." The contract employee shall promptly return PIV card(s) to HUD as required by the Financial Acquisition Regulation Clause 52.204-9. The GTM/GTR shall notify the COR immediately when there is no longer a need for a contractor's HUD-issued PIV card (e.g., contract employee terminates employment with the Department or contract employee no longer requires access to HUD facilities). This clause directs GTM/GTR/COR's and the contract company to ensure that all PIV cards are returned to the HQ PIV office upon receipt.

4. The Administrative Officer or Program Office Representative of the separating employee must ensure the HUD 58/58A is submitted promptly via SEC to the Bureau of Fiscal Services, Personnel and Payroll Processing Unit, for reconciliation and disbursement of any lump sum payments that may be due to the employee. If the PIV card is not returned, it is considered a debt to the Department. If the employee is indebted to HUD, the cost of the PIV card will be deducted prior to making any disbursement.

5. The HQ Personnel Security/PIV Branch will label, "for destruction," received PIV cards of separating employees, update USAccess and other relevant security database, then, destroy those PIV cards.

CHAPTER 5. MISCELLANEOUS INFORMATION

This chapter includes miscellaneous information and requirements of the HUD's PSSP program.

5-1 Security and Suitability Process End-to-End Hiring Roadmap

OPM developed a Security and Suitability Process Roadmap (see Appendix A) for agency use on *covered positions* in the competitive service (as defined in 5 CFR §731) and career SES appointments. In addition, there is also a Referral Chart (see Appendix B) to assist agency adjudicators in determining which cases require referral to OPM for debarment consideration.

5-2 Requirements for Adjudicators

- Adjudicators must meet Performance Accountability Council (PAC) approved training requirements as directed by the Security and Suitability Executive Agents.
- National security adjudicators must be properly qualified, trained and meet the personnel security investigative and adjudicative standards for assignment to a critical sensitive position.

5-3 Personally Identifiable Information (PII)

- The Privacy Act of 1974, (5 USC § 552a), as amended, and the E-Government Act of 2002 (Public Law 107-347), as amended, are the two primary laws that direct federal agencies responsibilities of protecting and securing personal information.
- These laws regulate the collection, maintenance, use, and dissemination of personal information in government records when that information is retrieved by the name or other personal identifier of the subject of record.
- All HUD users of PII must provide appropriate protection of information contained in, or extracted from, paper files or automated systems.

5-4 Personnel Security Record Requirements

- The Security Controlled Automated Tracking System (SCATS) is the primary electronic storage medium for personnel security records maintained by HUD.
- Original signatures are not required; electronic or facsimile copies are acceptable for personnel security release forms, such as the Standard Form (SF) releases, unless required by Executive Order or OPM guidance.
- Hard copy personnel security case files and background investigations are stored in an approved combination-locked cabinet or General Services Administration (GSA) safe or equally secure area, and stored in accordance with PII and classified document regulations. Any disclosures of information outside of HUD from background

investigation files are made in accordance with appropriate laws, regulations, or the HUD Privacy Act.

5-5 Records Retention

Pursuant to the current records schedule, HUD personnel security records are retained and destroyed in accordance with General Records Schedule (GRS) 18, item 22a and 22c, approved by the National Archives and Records Administration, the OPM Central-9 records as recorded in the Federal Register and the DHS-023 Systems of Records Notice (SORN). Records are destroyed upon notification of death or not later than five years after separation or transfer of employee, whichever is applicable, except in instances of ongoing litigation. Records in the personnel security case files are destroyed with the related case.

5-6 Fingerprints

- Fingerprints are required for all initial investigations; reinvestigations where the initial investigation is out of scope, causing a new initial investigation; and some reinvestigations where fingerprints provide required information to resolve issues.
- Electronic fingerprinting methods are preferred for automation and reporting purposes.
- Fingerprint capture establishes a biometric chain of trust by using the prints as part of the background investigation for PIV credentialing and system/facility access.

5-7 Freedom of Information Act (FOIA) and/or Privacy Act (PA)

An individual may request, under the provisions of the Privacy Act and/or FOIA, copies of their own background investigation by submitting a request to the FIS FOI/PA office using the INV100 Freedom of Information, Privacy Act Record Request Form (PDF file) [196.45 KB] or submit a handwritten request. Requests can be sent to the OPM-FIS FOI/PA office via the methods listed below:

Mail to:

FOI/PA office
OPM-FIS
PO Box 618
1137 Branchton Road
Boyers, PA 16018-0618

OR

E-mail: FISFOIPARequests@opm.gov

5-8 Use of Technology

Information technologies implemented to support personnel security processes utilize the proper technical safeguards, user training and assessments (e.g., privacy, certification and accreditation) to ensure adequate protection of personnel security related information.

5-9 Quality Assurance

Processes that should be tracked in a quality assurance program consist of all metrics in the investigations process, which can be used to ensure quality, accurate and timely products in compliance with Federal Investigative Standards. This includes tracking specific metrics and implementing specific quality review processes in anticipation of government-wide investigations performance standards as set by the Security and Suitability Executive Agents.

APPENDICES

Appendix A: OPM's Security and Suitability End-To-End Hiring Roadmap found at:

(https://www.opm.gov/policy-data-oversight/human-capital-management/hiring-reform/securitysuitabilityelements.pdf)

ELEMENTS AND TASKS

Validate Need for new position against the Workforce, Staffing and Recruiting Plans.

Ownership: Managers

Maximum number of calendar days: (refer to Hiring Process Roadmap)

Confirm Accuracy/Reconcile Position Description

Ownership: Managers, Human Resources Office

Maximum number of calendar days: (refer to Hiring Process Roadmap)

Designate Position using OPM-provided Position Designation System, which will automatically Determine Level of Investigation Commensurate with Position Designation

Ownership: Human Resources Office or Security Office with input from Managers

Maximum number of calendar days: 1

Best Practice: Managers provide input to the office designating the position.

- Designate the sensitivity level for the position, which triggers the investigative requirements for the position in relation to the national security assessment required by 5 CFR § 1400.
- Designate the risk level for the position. Suitability investigative requirements pursuant to 5 C.F.R. part 731 vary according to the position's potential for adverse impact to the efficiency or integrity of the service.
- Designations must not be influenced by the cost of the investigation entailed.

Note: Ongoing initiatives of the Joint Reform Team may impact current investigative solutions.

Identify candidate and extend offer of employment

Ownership: Human Resources Office

Maximum number of days: (Refer to Hiring Roadmap)

- Offer may be conditional based on subsequent determinations that the person is suitable for Federal employment and that the person's appointment is clearly consistent with the interests of the national security at the sensitivity level designated.
- Offer may be conditional based upon a subsequent finding that the person is eligible to have access to classified information at the required level.

Review the candidate's Declaration for Federal Employment (required for new employees), Optional Form (OF) 306. Look for issues that might be considered a basis for finding an individual unsuitable for Federal employment. Agencies have the discretion to decide who will have the responsibility for reviewing the Declaration for Federal Employment; however, this important step should not cause delays and may require increased communication between field locations, HR and Security offices (depending on agency structures).

Ownership: Human Resources Office or Security Office

Maximum number of calendar days: Refer to Hiring Process Roadmap

- If issues relating to material, intentional false statement or deception or fraud in examination or appointment appear to be present, refer to OPM.
- If issues relating to failure to testify as required pursuant to 5 C.F.R. § 5.4 appear to be present, refer to OPM.
- If suitability issues involving something other than those mentioned above, the agency should refer to OPM's suitability referral guidelines to determine whether the case should be referred to OPM, or adjudicated under the agency's delegated suitability authority.

If examination of the OF-306 is favorable, determine if there is a current investigation and/or adjudication that may satisfy investigative or adjudicative requirements under reciprocity rules and whether a valid Federal identity credential can be verified.

Ownership: Human Resources Office and Security Office

Maximum number of calendar days: 1 day, if there is a decision that can be reciprocally accepted. If the decision is not reciprocally accepted, the maximum number of days can extend to 6 months or more, as agencies respond to file requests from other agencies with varying response times.

- Security office (**PSD)** will search Clearance Verification System (CVS) and OPM Security/Suitability Investigations Index (SII) for investigations.
- The planned enhancements to CVS include display of HSPD-12 credential information.

If no current investigation, Initiate Request for Investigation

Ownership: Security Office **(PSD)**

Maximum number of calendar days: 10

- Agency ensures candidate has completed appropriate investigative questionnaire using the Electronic Questionnaire for Investigations Processing (e-QIP) and provided certification and releases. e-QIP is the most efficient means for submitting investigative requests.
- If OPM is the investigative service provider, agency completes Agency Use Block and indicates whether advance results of FBI National Criminal History Check (fingerprint check) or advance results of National Agency Check (NAC) are desired (for interim personal identification verification credential issuance, advance employment determination and/or interim clearance determination).
- Agency reviews the OF-306 and resumes assessing consistency with investigation request questionnaire; material, intentional false statement or deception in examination or appointment is reported to OPM FISD Suitability Adjudications Branch.

If OPM will be the investigative service provider, agency submits investigative request package in accordance with OPM guidance contained in publication INV-15 (formerly IS-15) "Requesting OPM Personnel Investigations." If new request for investigation has been initiated, agency may make an interim credentialing consistent with Government-wide guidance. Interim clearance decisions and interim appointment decisions can also be made at this point**.**

Ownership: Security Office or Adjudicating Official

Maximum number of calendar days: 3 (if favorable results of NAC or Fingerprint check)

- Requires appropriate identity source documents from applicant and results of NAC or Fingerprint check.
- Agency will utilize "Final Credentialing Standards for Issuing Personal Identity Verification Cards under HSPD-12" released by OPM July 31, 2008 or any successor standards that may be issued in the future. These standards apply to Executive agencies under E.O. 13467. Where a credentialing determination is not automatic based on reciprocity, the agency may make either an interim credentialing determination or a single and final credentialing determination, as described in the Standards.

The employee may enter on duty if the agency desires, in advance of investigation completion and final adjudication, depending on position sensitivity and whether pre-appointment investigative requirements may be temporarily waived.

Ownership: Human Resources Office and Security Office

- Waiver of the pre-appointment investigative requirement for Sensitive positions is restricted as described in 5 CFR § 1400.202. Note: waivers may be granted for Critical-Sensitive positions or Noncritical-Sensitive positions. The pre-appointment investigative requirement may not be waived for appointment to positions designated Special-Sensitive.

OPM screens completed investigations for jurisdiction regarding issues that could result in debarment from Federal employment.

Ownership: OPM

Maximum number of calendar days: 1-21 days, depending on type of investigation and notifies agency of results.

- If such indicators are present, OPM retains report of investigation, makes suitability adjudication and notifies agency of results.
- If unfavorable adjudication by OPM, OPM notifies agency and notifies individual of appeal rights to the Merit Systems Protection Board.

If investigation not retained for adjudication by OPM, then Adjudicate Investigation

Ownership: Agency Adjudicating Official

Maximum number of days for Clearance Adjudication - 90% within 30 days (FY08), 90% within 20 days (FY09 and beyond); Maximum number of days for suitability determination-only has not been stipulated but may be defined as reform initiatives align security and suitability processes.

- The "Credentialing, Suitability and Security Clearance Decision-Making Guide" released by OPM in January 2008 may assist in agency decision-making.
- The agency suitability and/or security adjudication provides the *de facto* final personal identification verification credentialing determination.

If favorable adjudication and employee has not yet entered on duty, Employee Enters on Duty

Ownership: Human Resources Office

Maximum number of days: (refer to Hiring Process Roadmap)

Appendix B: Referral Chart
Information Requirements for Suitability Referrals

This chart was created by OPM at the following web address:
https://www.opm.gov/investigations/background-investigations/suitability-adjudications/#url=Referral-Chart

Issues	Criteria
• Any evidence of dishonesty or fraud in the competitive examination or appointment process (such as falsification of application)	Always refer, regardless of the date of occurrence
• Any statutory debarment issue • Any loyalty or terrorism issue	Always refer, regardless of the date of occurrence
MAJOR & SUBSTANTIAL ISSUES, including but not limited to: • Patterns of conduct (such as a pattern of drug or alcohol abuse, financial irresponsibility or major liabilities, dishonesty, unemployability for negligence or misconduct, criminal conduct) • Other than honorable military discharge • Felony offense • Illegal drug manufacturing, trafficking, or sale • Major honesty issue (such as extortion, armed robbery, embezzlement, perjury) • Serious violent behavior (such as rape, aggravated assault, arson, child abuse, manslaughter) • Sexual misconduct (such as sexual assault, sexual harassment, prostitution) • Illegal use of firearms or explosives • Hatch Act violation • Employment related conduct involving dishonest, criminal, or violent behavior	Refer all within 3 years *For patterns, the conduct may begin prior to, but must extend into, the last 3 years*
MODERATE ISSUES, including but not limited to: • Driving while intoxicated • Drug-related offense (excluding infrequent use or possession of marijuana or marijuana paraphernalia , to include arrests or charges for possession of marijuana) • Petty Theft or Forgery • Assault, criminal mischief, harassment • Employment related misconduct involving insubordination, absenteeism, rules violations	Refer for 2 or more occurrences within 3 years *May be a combination of Moderate and Minor issues within 3 years*

Information Requirements for Suitability Referrals

This chart was created by OPM at the following web address:
https://www.opm.gov/investigations/background-investigations/suitability-adjudications/#url=Referral-Chart

Issues	Criteria
MINOR ISSUES, including but not limited to: • Minor liquor law violation • Minor traffic violation • Bad check • Minor disruptive conduct (such as disorderly conduct, trespassing, vagrancy, loitering, disturbing the peace) • Minor employment related misconduct	Refer for 3 or more occurrences within 3 years *May be a combination of these issues within 3 years*

Appendix C: Appeal Procedures for

Suspension, Denial, or Revocation of a Security Clearance and Access to Classified Information

The following appeal procedure applies to all HUD Federal employees holding a National Security Clearance and creates no procedural or substantive rights.

Denial or Revocation of Security Clearance

Pursuant to the Adjudicative Guidelines, any doubt as to whether access to classified information is clearly consistent with national security will be resolved in favor of the national security to protect the best interest of the agency and the federal government.

Deciding Authority

HUD review officials for personnel security determinations regarding suspension, revocation, denial, granting, or reinstatement include:

1. First-Level Deciding Authority**:** The Director of the Personnel Security Division.
2. Second-Level Deciding Authority: The supervisor of the First-Level Deciding Authority, who is the Director for Human Capital Services.
3. Third-Level Deciding Authority: The Security Appeals Board. For each denial or revocation matter, the Board is comprised of three agency personnel granted a national security clearance at or above the level, of the the subject making an appeal, and appointed by the Secretary or his or her designee. Two of these members are selected from outside the security field.. The Board's decision is Final.

The following procedural requirements apply when a HUD Federal employee, with a National Security Clearance and/or Secret Compartmented Information (SCI) access has been denied access to classified information or has had their access to classified information revoked:

Notice of Determination

A. The First-Level Deciding Authority provides a written Notice of Determination that:

(1) Informs the individual that his or her access to classified information has been denied or revoked.

(2) Includes a written explanation for the determination to the extent permitted by law, as required by E.O. 12968.

(3) States the name and office address of the Second-Level Deciding Authority to whom the individual should direct any reply, request, or filing.

(4) Informs the individual of his/her right to be represented by counsel or other representative at his or her own expense.

(5) Advises the individual that he/she may request documents, records, and reports upon which the denial or revocation was based; and/or request a copy of the entire investigative file, as permitted by the applicable laws and regulations, including E.O. 12968.

a. These documents, records, and reports must be requested no later than fifteen (15) calendar days following the receipt of the Notice.

b. If requested, the documents, records, and reports are made available to the extent they would be available if requested under the Freedom of Information Act, 5 USC Section 552, as amended, or the Privacy Act of 1974, 5 USC Section 552a, as amended, and as permitted by national security and other applicable laws.

(6) Advises the individual that he/she may reply in writing and may request a review of the determination.

a. If the individual requests documents, records, or reports, the written reply must be submitted within thirty (30) calendar days of the date of final notification that all documents relied upon have been provided.

b. If the individual does not request documents, records, within thirty (30) calendar days of the date of the Notice of Determination, the denial/revocation decision becomes final.

(7) Advises the individual that he/she may request to appear personally, or via telephone or teleconference, before the Second-Level Deciding Authority and to present relevant documents, materials, and information at that time. A request to appear personally must be made within thirty (30) calendar days following the date of the Notice of Determination, or thirty (30) calendar days from the date of final notification that all documents relied upon have been provided if the individual requested documents, reports, or records.

a. Travel expenses and any associated costs are incurred by the individual.

b. The individual and his or her representative, the second-level deciding authority, counsel advising the component, and administrative support personnel requested by the Second-Level Deciding Authority are permitted to attend the personal appearance.

c. A written summary or recording of such appearance is included as part of the individual's security file within the PSD.

(8) Advises the individual that if no response is provided regarding the Notice of Determination within the specified time-period, PSD will make a determination based solely on the information relied upon. The Notice of Determination becomes final without further notice.

B. In the case of an employee, the First-Level Deciding Authority notifies the individual's supervisor(s) of the denial or revocation and advises the supervisor of his/her responsibility for ensuring that the individual not have access to classified information during the denial or revocation process.

Notice of Review

A. The Second-Level Deciding Authority reviews the record in the case including the Notice of Determination, any documentation on which the Notice of Determination is based, the written reply, the personal appearance (if any), and any documentation provided.

B. Upon completion of the review, the Second-Level Deciding Authority provides a written decision to the individual and/or his or her representative, in accordance with E.O. 12968. The Notice of Review advises the individual of the decision to reverse or to uphold the Notice of Determination:

(1) If the decision is to reverse the Notice of Determination, the Notice will provide the reason for the reversed determination.

(2) If the decision is to uphold the Notice of Determination, the Notice of Review informs the individual that he or she has fifteen (15) days from the date of the Notice of Review to file an appeal in writing with the Security Appeals Board. The Notice of Review would inform the individual to address the written appeal to:

Department of Housing and Urban Development
Attn: Personnel Security Appeals Board
451 7th Street SW
Washington, DC 20410

The individual sends a copy to the Second-Level Deciding Authority.

(3) Extensions of time to appeal the Notice of Review are not granted by the Security Appeals Board absent compelling circumstances.

C. When a notice of appeal is submitted, the Second-Level Deciding Authority forwards materials pertinent to the underlying denial or revocation matter to the Security Appeals Board through the HUD Personnel Security Division.

Specific Criteria for Granting Secret/Top Secret Clearances and/or Access to SCI:

Prior to HUD granting a SECRET/TOP SECRET clearance, the Personnel Security Division requires a formal written agreement (Position Description) that the HUD employee requires a clearance.

The HUD SCI program is solely governed by the Central Intelligence Agency (CIA). All SCI requests are forwarded to the CIA for action via HUD PSD protocols.

Appendix D: Acronym Reference Sheet

1. BFS – Bureau of Fiscal Services (HUD's current HR service provider)
2. CFR – Code of Federal Regulations
3. CVS – Central Verification System
4. DHS – Department of Homeland Security
5. E.O. – Executive Order
6. e-QIP – Electronic Questionnaire for Investigations Processing
7. FIN – Federal Investigative Notice
8. FISD – OPM's Federal Investigative Services Division
9. FOIA – Freedom of Information Act
10. GRS – General Records Schedule
11. HR – Human Resources
12. HSPD-12 – Homeland Security Presidential Directive 12
13. IDMS – Identity Management Service
14. IRPTA – Intelligence Reform and Terrorism Prevention Act of 2004
15. MBI – Moderate Risk Background Investigation
16. NACI – National Agency Check with Inquiries
17. ODNI – Office of the Director of National Intelligence
18. OMB – Office of Management and Budget
19. OPM – Office of Personnel Management
20. PA – Privacy Act
21. PAC – Performance Accountability Council
22. PDT – Position Designation Automated Tool
23. PIV – Personal Identity Verification
24. PSD – Personnel Security Division
25. PSSP – Personnel Security and Suitability Program
26. SAVE – Systematic Alien Verification System
27. SCATS – Security Controlled Automated Tracking System
28. SORN – System of Records Notice
29. USCIS – United States Citizenship and Immigration Services
30. VRA – Veteran's Readjustment Act