HHS

PERSONNEL SECURITY/SUITABILITY

HANDBOOK

SDD/ASMB 1/98

PERSONNEL SECURITY/SUITABILITY HANDBOOK

CONTENTS

PERSONNEL SECURITY/SUITABILITY HANDBOOK

This handbook is for the use of HHS officials who have personnel security or suitability responsibilities. The handbook contains procedures and guidance for the Department's personnel security program which is outlined in Personnel Instruction 731-1. It is to be used primarily by the staff of the Security and Drug Testing Program Division (SDD), ASMB, and OPDIV and STAFFDIV Personnel Security Representatives (PSRs). Employees in servicing personnel offices who schedule and adjudicate personnel background investigations and Information Security Officers also should use this handbook to assist them in handling their personnel security responsibilities.

The Personnel Security/Suitability Handbook is prepared and updated by the Director, SDD. Questions, concerns, requests, or suggestions should be directed to that office within ASMB. Immediate changes in procedures and/or requirements are brought to the attention of PSRs through written or automated memoranda. Changes to the handbook are made on an "as needed" basis.

Definitions

A. Automated Information System - Any organized collection, processing, transmission, and dissemination of information in an automated format, also referred to as a computer or ADP system.

B. Classified Information - National security information that is so designated pursuant to the three levels of classification as defined in Executive Order 12958, Classified National Security Information, and referred to as Top Secret, Secret, or Confidential.

C. Contractor - Any individual (industrial, commercial, or other entity) who has executed a contract with the Department (or one of its components) for the purpose of performing work in support of departmental goals, objectives, programs, and/or services. In determining whether a contractor is subject to investigative requirements, a contractor in most cases will either work in HHS-owned or leased space, or will have access to HHS equipment or protected data. A contractor also can be a

subcontractor to a HHS contractor.

D. Credit Check - This is an automated credit record search conducted through various major credit bureaus. It is included in most background investigations except the basic NACI investigation required of employees entering Non-Sensitive (Level 1) positions.

E. National Security Positions - Sensitive positions (designated as Level 2, 3, or 4)in which the incumbents' duties and/or responsibilities involve access to classified information or other restricted information relating to the security of our nation.

F. Non-Sensitive Positions - Positions (designated as Level 1) which are neither Public Trust nor National Security positions.

G. Position Sensitivity - The degree of risk and level of relative importance assigned to a specific position.

H. Public Trust Positions - Positions (designated as Level 5 or 6) in which the incumbents' actions or inactions could diminish public confidence in the integrity, efficiency, or effectiveness of assigned Government activities, whether or not actual damage occurs; and positions in which the incumbents are being entrusted with control over information which the Department has legal or contractual obligations not to divulge.

I. Security Clearance - An administrative determination based upon the results of a favorably adjudicated background investigation that an individual is trustworthy and may be granted access to a specified level of classified national security information as required in the performance of assigned duties.

J. Special Agreement Checks (SAC) - A special agreement between the Office of Personnel Management's Office of Federal Investigations (OPM/OFI) and a department or agency which provides for OPM/OFI to conduct special specific record checks at nominal cost.

K. Suitability - General fitness or eligibility for Federal employment.

Responsibilities

Personnel security/suitability responsibilities are shown below:

A. The Assistant Secretary for Management and Budget (ASMB)

Under the authority delegated by the Secretary, the ASMB is responsible for:

1. Administering the Department's personnel security/ suitability program in accordance with the provisions of EO 10450 and 5 CFR Parts 731, 732, and 736.

2. Deciding whether to approve the waiver of the required preappointment investigation of an individual who is going into a highly sensitive National security (Level 3) or high risk Public Trust (Level 6) position.

3. Retaining jurisdiction over all personnel security cases, prior to submission to the Secretary, involving a potential determination that any employee should be suspended, reassigned, or terminated in the interest of the national security.

B. Heads of OPDIVs and STAFFDIVs are responsible for:

1. Determining the sensitivity level of all positions within their areas of responsibility and assuring required background investigations are conducted.

2. Establishing effective methods for assuring that consistent, timely, and equitable adjudicative determinations are made on all personnel security/ suitability cases involving their employees and contractors.

3. Referring loyalty or national security matters to the ASMB for evaluation and/or investigation.

4. Designating an official to serve as their Personnel

Security Representative (PSR) to handle those responsibilities listed in the *HHS Personnel Security/ Suitability Handbook*.

C. The Deputy Assistant Secretary for Human Resources (DAS/HR)

Under the executive direction of the ASMB, the DAS/HR is responsible for overseeing and evaluating HHS personnel security/suitability policies and programs.

D. The Director, Personnel Security and Drug Testing Program Division (SDD)

Under the general direction of the Deputy Assistant Secretary for Human Resources, ASMB, the Director, SDD, is responsible for:

1. Developing, implementing, and evaluating Departmental personnel security/suitability policies and programs.

2. Providing program improvement recommendations through periodic assistance and evaluation visits to OPDIV and STAFFDIV offices to ensure that the basic responsibilities of EOs 10450 and 12968; 5 CFR 731, 732, and 736; and Departmental personnel security and suitability directives are being met.

3. Providing consultation, advice, and written instructions or guidance relating to the Department's personnel security/suitability program, to include the HHS Personnel Security/Suitability Handbook.

4. Establishing and maintaining personnel security files for HHS employees and contractors in national security and public trust positions.

5. Requesting personnel investigations from the Office of Personnel Management (OPM) when required for employees and contractors in national security and public trust positions.

6. Adjudicating reports of investigation which are favorable and do not require referral to a Personnel Security Representative (PSR).

7. Directing reports of investigation to the appropriate

PSR when necessary for review and adjudication.

8. Issuing security clearances to HHS employees and contractors based upon an identifiable need and a favorable report of investigation.

9. Establishing internal SDD operating procedures in accordance with OPM policy and 5 CFR Part 736 for the handling and safeguarding of sensitive unclassified reports of investigation to protect the interests of both the individual and the Department.

E. Personnel Security Representatives (PSRs) are responsible for:

1. Assuring that correct and consistent position sensitivity levels are designated for all their OPDIV or STAFFDIV positions and that the correct sensitivity level codes are shown on personnel and security forms requiring their review.

2. Submitting to the Director, SDD, any request for a waiver of a required preappointment investigation and requests for required investigations and reinvestigations of employees, applicants, and contractors who will be or are occupying National Security or high risk Public Trust positions.

3. Adjudicating reports of investigation provided by the Director, SDD, or OPM, to resolve personnel security/suitability issues; or delegating the adjudication responsibilities to the Servicing Personnel Officer (SPO) or other designated official.

4. Forwarding the Certification of Investigation notice and any approved waiver request to the SPO for required filing in employee's Official Personnel Folder (OPF).

5. Ensuring, when adverse actions are considered, that due process procedures are followed and that such actions are coordinated with the SPO, supervisor, and Office of General Counsel (OGC) attorney, as necessary.

6. Approving any request for a security clearance for

access to classified information, using HHS 207 form, prior to submitting it to the Director, SDD.

7. Assuring that each employee and contractor subsequently granted a security clearance receives a briefing on security matters and that the signed briefing form is forwarded to SDD.

8. Assuring that each individual having a security clearance is debriefed when access to classified information is no longer needed and that SDD is promptly notified of this action.

9. Notifying SDD when employees or contractors in National Security or high risk Public Trust positions leave HHS.

10. Providing to the Director, SDD, any requested personnel security/suitability data and/or reports in a timely manner.

11. Assuring that their top management officials are kept informed of pertinent personnel security/suitability matters and coordinating actions with the SPO(s).

12. Referring to the Director, SDD, any developed unfavorable personnel security/suitability information on an employee, applicant, or contractor being considered for or occupying a National Security or high risk Public Trust position.

F. Servicing Personnel Officers (SPOs) are responsible for:

1. Ensuring that investigative requirements for each position filled are met and that any required waiver has been approved.

2. Initiating required requests for National Agency Check and Inquiries (NACI) investigations directly to OPM on all appointees to Non-Sensitive (Level 1) positions.

3. Ensuring that the proper security questionnaire and fingerprint card are completed by any individual selected for a national security or public trust position prior to forwarding them to the appropriate PSR with any other forms necessary for scheduling the background investigation.

4. Referring unfavorable personnel security and suitability information to the appropriate PSR, and coordinating actions with the office supervisor, OGC attorney, and Director, SDD, as necessary.

5. Ensuring that the decision to reemploy a person who resigned from another Federal agency is based upon complete and pertinent personnel security information.

6. Assisting applicants, employees, contractors and supervisors in understanding and/or preparing any required personnel security questionnaires or forms.

7. Fingerprinting, and reprinting when necessary, employees or contractors who require investigations.

8. Adjudicating the NACI reports of investigation on individuals in Non-Sensitive (Level 1) positions or handling other adjudication responsibilities delegated by the PSR.

9. Assuring that the Certification of Investigation notice and any approved waiver form are filed in the OPF when required.

G. Immediate supervisors are responsible for:

1. Ensuring that employees promptly submit any required investigative forms to the appropriate PSR or SPO.

2. Promptly providing to the appropriate PSR or SPO acquired unfavorable information regarding the conduct or behavior of a subordinate which indicates possible suitability or national security concerns.

3. Ensuring that positions under their purview are designated at the proper sensitivity level.

Descriptions of Investigation Types

Described below are the types of investigations offered and conducted by the Office of Personnel Management (OPM) and its privatized contractor, the US Investigations Services, Inc. (USIS).

National Agency Check (NAC) - An integral part of all background investigations, the NAC consists of searches of OPM's

Security/Suitability Investigations Index (SII); the Defense Clearance and Investigations Index (DCII); the FBI Identification Division's name and fingerprint files, and other files or indices when necessary.

National Agency Check and Inquiries (NACI) - This is the basic and minimum investigation required on all new Federal employees. It consists of a NAC with written inquiries and searches of records covering specific areas of a person's background during the past five years. Those inquiries are sent to current and past employers, schools attended, references, and local law enforcement authorities.

NACI and Credit (NACIC) - This NACI includes the addition of a credit record search and is the minimum investigation for those going into low risk public trust positions (Level 5)

Access NACI (ANACI) - This is a new investigation designed as the required initial investigation for Federal employees who will need access to classified national security information at the Confidential or Secret level. The ANACI includes NACI and Credit coverage with additional local law enforcement agency checks.

Child Care NACI (CNACI) - OPM has an agreement with HHS to conduct this enhanced NACI that includes a search of records of state criminal history repositories of the state where the subject resides. This investigation is designed to meet special investigation requirements for those who are in child care provider positions.

NAC with Local Agency Check and Credit (NACLC) - This is a new investigation which is the same as the ANACI without the written inquiries to past employers, schools attended, etc. It is designed as the initial investigation for contractors at the Confidential and Secret national security access levels. The NACLC also is to be used to meet the reinvestigation requirement for all individuals (including contractors) who have Confidential or Secret clearances.

Minimum Background Investigation (MBI) - This investigation includes a NACI, a credit record search, a face-to-face personal interview between the investigator and the subject, and telephone

inquiries to selected employers. The MBI is an enhanced version of the NACIC and can be used for selected public trust positions.

Limited Background Investigation (LBI) - This investigation consists of a NACI, credit search, personal subject interview, and personal interviews by an investigator of subject's background during the most recent three years.

Background Investigation (BI) - This is a more in depth version of the LBI since the personal investigation coverage is the most recent five to seven years. This investigation is required of those going into highest risk public trust positions (Level 6).

Single Scope Background Investigation (SSBI) - This is the government-wide investigation required of those who need access to Top Secret classified national security information. This background investigation covers the past seven years of the subject's activities (or to age 18, whichever is less). It includes verification of citizenship and date and place of birth, and well as national agency records checks on the subject's spouse or cohabitant, interviews with selected references and former spouses.

SSBI-Periodic Reinvestigation (SSBI-PR) - This is the required five year update investigation for those who have Top Secret security clearances. It consists of personal investigative coverage of employments and residences since the previous investigation, including interviews with all former spouses divorced during the coverage period. A search of the Treasury Department's financial data base is also to be included.

Position Sensitivity - Guidance and Procedures

There are three position sensitivity designations (Non-Sensitive, Public Trust, and National Security) which correlate with six specific sensitivity levels (Levels 1 through 6). Determining whether a position has specific national security or public trust responsibilities is the key to designating the sensitivity level. This is because national security positions are automatically designated one of three levels (2, 3, or 4), and public trust positions are designated as either Level 5 or 6. Without these special responsibilities, positions are designated as Non-Sensitive, which is Level 1. (see below)

Non-Sensitive	National Security	Public Trust
Level 1	Level 2, 3, or 4	Level 5 or 6

The easiest way to determine the sensitivity of a position is first to decide whether a security clearance is required of the incumbent. If the previous occupant of the position required access to classified national security information, then the position should be considered a National Security Position. Use the chart below to determine the sensitivity level by matching up with the level of security clearance required. **If no security clearance is required or anticipated, skip down to number 2. Public Trust Positions.**

1. National Security Positions

   At HHS, National Security Positions are those in which the incumbent needs a security clearance for access to classified national security information. These can be a variety of positions, but the key attribute is that the position requires the regular use of, or access to, classified information.

   If a security clearance is required, the sensitivity level is as follows:

Type of Clearance =	Sensitivity Level(formerly called)
CONFIDENTIAL or SECRET	Level 2 (Non-Critical Sensitive)
TOP SECRET or (DOE's) Q	Level 3 (Critical-Sensitive)
Special Access (or Presidential Appointee)	Level 4 (Special-Sensitive)

2. Public Trust Positions

   Security clearances are quite limited at HHS but public trust responsibilities are much more prevalent and should be evaluated as the next step in the designation process. Although the public expects all Federal employees to be trustworthy and honest, positions designated as Public Trust Positions are those requiring a much higher degree of integrity with unwavering public confidence in the individual occupying the position. Public Trust Positions include those

involving policymaking, major program responsibility, and law enforcement duties. Also included are those involving access to or control of unclassified sensitive or proprietary information or financial records, and those with similar duties through which the incumbent can realize a significant personal gain or cause very serious damage.

At HHS, many of our employees and contractors who have access to our computer data systems should be in positions designated as public trust.

The public and the Department are put at risk if the incumbent does not meet the high standards of integrity and confidence required of those in Public Trust Positions. OPDIV and STAFFDIV management must decide which of their positions have these enhanced public trust responsibilities and thus should be designated as Public Trust Positions. Management must further decide the relative degree of risk, moderate or high, inherent in these public trust positions so that they can assign a designated sensitivity level of 5, for moderate risk, or level 6, for high risk.

To promote consistency, effectiveness, and ease of operation within the Department, some personnel security and ethics program designations are being linked. The ethics program regulations require that employees in specific designated positions file an annual financial disclosure report (SF 278 or OGE 450) to ensure confidence in the integrity of the Federal government by demonstrating that they are able to carry out their duties without compromising the public trust. By definition, these designated filers of an annual financial disclosure report occupy public trust positions and, for personnel security purposes, their positions shall be designated as Public Trust Position Level 5 or 6, unless they meet the criteria for a National Security Position as stated above.

Therefore you should use the ethics program designation as your initial step in determining whether a position is a Public Trust Position. If the incumbent of the position is required to file either annual financial disclosure report, then the incumbent is in a Public Trust Position. The Department maintains lists of these designated positions which

are reviewed annually to assure that only positions which meet strict filing criteria are included.

Although these positions are by definition "public trust positions", management still makes the most important personnel security decision in deciding the relative risk level, moderate or high (Level 5 or 6). This is the most important decision because the background investigation required of these two levels differs considerably in coverage and cost.

The required investigation of most entrants into a Level 5 public trust position is minimal, usually nothing more than a credit bureau check in addition to the regular required NACI investigation done on new hires. However, the credit check provides much information to aid management in deciding whether there is a risk in placing the individual in a public trust position. The required Background Investigation (BI) on an individual in a Level 6 position is a costly one with several years of coverage.

Public trust positions, following the designation criteria in the ethics program guidance, include positions encumbered by the following officials: (not all-inclusive)

> SES members, Schedule C appointees, administrative law judges, most commissioned corp officers, GS-13 to 15 officials who are substantially involved in contracts, procurements, grants, or responsibilities involving a high risk for conflict of interest.

In addition to the "predesignated" Public Trust Positions, others meeting the definition must be designated as either Level 5 or 6. They should include positions having the following duties: law enforcement, investigations, audit, security, and access to sensitive, proprietary, or financial information, including access through, and/or control over, automated information systems (computer data systems).

In deciding if a Public Trust Position has risks at the high level (6), remember that Level 6 requires a BI, and is best reserved for positions where information about the incumbent's entire background is very important, e.g., in law enforcement, investigator, and security positions. If in doubt, designate at Level 5, however, require a LBI or another more thorough investigation above the minimum NACI and Credit.

3. Non-Sensitive Positions

The majority of HHS positions are Non-Sensitive (Level 1) because the mission of the Department involves mostly low risk, non-sensitive, and non-national security program responsibilities. After having considered national security and public trust responsibilities, those remaining positions are considered Non-Sensitive.

A Non-Sensitive Position could move to a higher level if, e.g., the incumbent suddenly needed a Secret security clearance for an assigned duty. In that case the position would move to Level 2 and the incumbent would have to meet the investigative requirements for the Secret clearance level. If the clearance was not needed later, the position would revert to a Non-Sensitive Position (Level 1).

Another example of movement to a higher level of sensitivity could be if an employee in a Non-Sensitive Position is given responsibility over a contract and is therefore required to file an annual financial disclosure report. At the time of the assignment of the additional financial responsibilities, the position would convert to a Public Trust Position (probably Level 5). The employee would then need to meet Level 5 investigative requirements. In this example, the employee would probably need to complete the public trust security questionnaire (SF 85P) and be subject to a credit check.

Documentation of the rationale underlying designation decisions involving Public Trust Positions must be retained for audit purposes. However, separate documentation is not needed for those "predesignated" as public trust if the incumbents are required to file annual financial disclosure reports. The documentation can be a written statement explaining the reasoning for including a specific position, or group of positions, at a particular public trust level. (For example, the documentation statement could say that all police officer positions, 083 series, are designated as Level 5 and, because of their unique law enforcement responsibilities, new police officers are subject to a LBI.)

The documentation for National Security Positions is the security clearance request form (HHS 207) so further documentation is not needed.

The numerical sensitivity level (1-6) is the coding to be used on all security questionnaires (SFs-85, 85P, and 86) and on various personnel forms, e.g., the Position Description (OF-8), and SFs 50 and 52. This sensitivity code is also required to be shown for every employee in the automated personnel system (IMPACT).

What is most important when designating position sensitivity levels, and when determining which optional investigation to request, is to exercise good judgment, using risk management decision-making skills, and consistency.

Suitability Determinations

The "suitability" or "fitness" decision is arrived at by a process which involves the following actions:

1. The OPDIV or STAFFDIV assigns a sensitivity level to the position to be encumbered by an applicant, employee, or contractor.

2. OPM, or another Federal investigative agency, conducts a personnel background investigation as a prerequisite to determining whether the individual is suitable for employment for a specific position. The scope and coverage area of the investigation is determined by the sensitivity level assigned to the position. The investigation is designed to reveal pertinent facts, past and present, about the character, honesty, trustworthiness, reputation, etc., of the applicant, employee, or contractor.

3. OPM forwards the results of the background investigation to the security official whose name and address are obtained by using the Security Office Identifier (SOI) code. (That SOI code is on the top front of the security questionnaire and was entered there by whoever originally scheduled the investigation). The SOI contact official, usually the PSR, either adjudicates the suitability of the individual after reviewing the investigative materials provided, or requests additional investigative information, or requires the subject to provide more information or data necessary to permit adjudication.

4. The PSR may also forward the investigative materials to the SPO, or other designated official, for adjudication.

5. OPM forwards to SDD investigation reports conducted on individuals in all National Security and high risk Public Trust Positions. SDD reviews those reports and certifies the suitability of that person if the completed background investigation is favorable.

6. When the investigation report reveals unfavorable information, SDD (a) requires the appropriate PSR to provide any additional data necessary to permit adjudication by SDD

or (b) requests the PSR to adjudicate the suitability of that person and, if necessary, to coordinate the adjudication with SDD.

7. The criteria to use in making a suitability decision, including the specific factors to consider as a basis for finding an individual unsuitable for Federal employment, are found in 5 CFR Part 731.

8. The adjudicative process is the careful weighing of a number of variables known as the whole person concept. Available, reliable information about the person, past and present, favorable and unfavorable, should be considered in reaching a determination. The final suitability determination should be based on good judgement and common sense after consideration of all these variables.

9. The adjudicator should consider the following factors, in addition to those in 5 CFR Part 731, in serious issue cases:

   whether the person-

   (a) voluntarily reported the unfavorable information;

   (b) was truthful and complete in responding to questions;

   (c) sought assistance and followed professional guidance, where appropriate;

   (d) resolved or appears likely to favorably resolve the suitability concern, e.g. credit problems;

   (e) has demonstrated positive changes in behavior and employment.

10. Due process procedures must be followed when there is to be a proposed unfavorable determination. Guidance should be obtained from the Office of the General Counsel (OGC) and employee and labor relations staff. In most cases where there are suitability/security issues involved, the individual should be interviewed and given a opportunity to respond to those issues developed in the investigation. Sometimes that information is incorrect or incomplete and this interview allows the individual to learn what the investigative file shows. The interview is also a quick way to gather adjudicative information because the individual

can be asked to provide it, e.g., arrest disposition and credit record information.

Investigation Requirements

The minimum personnel background investigation requirements for the various position sensitivity levels are as follows:

Sensitivity Level	Minimum Investigation Required
NON-SENSITIVE **Level 1**	NACI (name & fingerprint checks & written inquiries)
NATIONAL SECURITY **Level 2** (Confidential or Secret clearance)	ANACI (Access NACI)
Level 3 (Top Secret clearance) **Level 4**	SSBI (Single Scope Background Investigation)*
PUBLIC TRUST **Level 5** (moderate) risk	NACIC (NACI + credit check)**
Level 6 (high risk)	BI (Background Investigation)*

* The investigation must be completed preappointment unless a waiver is approved. Preappointment requirement cannot be waived for Level 4.

** A MBI or LBI should be requested for specific Level 5 positions (such as law enforcement, audit, security, and non-career appointee positions) that are at a quite high risk level but are just under the Level 6 designation. These optional investigations provide more depth of coverage at an increased cost.

A. The required investigation must be initiated within 14 days of placement unless there is a preappointment investigation

requirement. When a waiver to that preappointment requirement is being requested for Levels 3 and 6, the completed investigation questionnaire (SF 86 or 85P) must accompany the request.

B. If the sensitivity level of occupied position changes due to realignment of duties or a requirement for a security clearance, an incumbent may remain in the position, but any investigation required by the new sensitivity level must be initiated within 14 working days.

C. If positions are being redesignated from Non-Sensitive to moderate risk Public Trust Positions to meet HHS guidelines, no additional investigation is necessary for incumbents who have had a NACI and been with HHS for at least one year. Employees with less than a year of employment with HHS, but who had a NACI, can meet moderate risk public trust requirements by having a credit check only conducted on them.

D. When an individual has been subject to a previous background investigation, it may not be necessary to request a new one,
especially if there has been no break in Federal service. A check of the individual's OPF (or SF 75, Request for Preliminary Employment Data) should show if the individual was previously investigated and the date and type of investigation. If investigation requirements have been met on an individual moving into a Public Trust or National Security Position, the PSR or SPO representative must notify SDD of the date and type of the previous investigation so SDD can set up the official security file. Investigative requirements are determined by OPM and SDD provides guidance.

E. The following Non-Sensitive Positions (Level 1) are exempt from the NACI investigation requirement of EO 10450, providing that reference checks are favorable and they are not child care provider positions:

(1) Intermittent, seasonal, per-diem, or temporary positions that do not exceed an aggregate of 180 days in either a single continuous or series of appointments (**includes most contractor positions**); and

(2) Aliens employed outside the United States

F. All incumbents of child care provider positions, including contractors, must meet the investigative requirements of PL 101-647, Section 408,"Child Care Worker Employee Background Checks", as amended by PL 102-190. The minimum required investigation is a NACI supplemented by state criminal history checks. OPM provides a specific investigation, a Child Care NACI (CNACI), which should be requested on individuals moving into child care provider positions. The investigation can be conducted post-appointment if the individual is under the supervision and in sight of a previously investigated staff person during anytime children are in the care of the newly hired individual.

The CNACI will also usually meet most investigative requirements of PL 101-630, Section 408, "Character Investigations" which covers individuals in positions requiring regular contact, with, or control over, Indian children. Most of these covered positions are also covered under the child care provider investigation requirement. The Indian Health Service (IHS) PSR provides guidance regarding these positions and the investigative requirements of PL 101-603.

G. The Director, SDD, and each PSR must assure that the analysis of background investigative information, the subsequent suitability/security determination, and the handling of the investigative reports follow the requirements, criteria, and standards in 5 CFR Parts 731, 732, and 736 and in EO 10450.

All pertinent information obtained from investigative reports, personnel records, responses to written inquiries, medical fitness records, personal or subject interviews, or any other sources, must be considered in reaching suitability/security determinations. Due process procedures must be followed when making an unfavorable determination.

Scheduling Investigations

OPM requires one of three completed security questionnaires for scheduling most of its investigations. Note that an individual is to complete the questionnaire only after a conditional offer of employment has been made. The three

questionnaires are:

SF 85 (Questionnaire for Non-Sensitive Positions)
Completed form to be forwarded to OPM by the SPO to request NACI investigations on **Level 1** positions.

SF 85P (Questionnaire for Public Trust Positions)
Completed form to be forwarded to SDD by PSR to request investigations for **Levels 5* or 6**.

SF 86 (Questionnaire for National Security Positions)
Completed form to be forwarded to SDD by PSR to request background investigations or reinvestigations for **Levels 2, 3, or 4**.

*For moderate risk Level 5 positions requiring only a NACIC investigation, the PSR forwards the SF 85P and other investigative forms (see below) directly to OPM. OPDIV PSRs should use their own assigned Security Office Identifier

(SOI) code on the SF 85P (not HE00, which is assigned to the Office of the Secretary (OS) and SDD) to ensure that OPM returns the completed investigation directly to them.

In addition note that the **SF 85P-S (Supplemental Questionnaire for Selected Positions)** is required to be completed by individuals going into law enforcement or security guard positions, and is to be attached to the SF 85P. SDD coordinates with PSRs in determining whether to require this form for other selected positions.

The **SF 86A (Continuation Sheet for Questionnaires SF 86, 85P and SF 85)** is to be used if additional space is needed for residence, education, and employment activities.

In addition to the SF 85P or 86, the complete investigation request package for SDD usually consists of:

1. One copy of the SF 85P or 86

2. One fingerprint card (SF 87; or FD 258, if contractor).

3. A resume or equivalent form if investigation is a part of employee's initial appointment action.

4. An **OF 306 (Declaration for Federal Employment)** is only required if the individual is receiving a new Federal

appointment. OF 306 is not required for reinvestigations or update/upgrade investigations.

All investigative questionnaire forms must reach OPM within 120 days of subject's signature and date.

A. Information on the questionnaires should be completed by the subject of the investigation. However, to avoid unnecessary delays in initiating investigations, sometimes it is necessary for the PSRs or the SDD staff to amend or complete certain items prior to forwarding the forms to OPM. OPM has created form **FIPC 391 (Certification of Amended Investigative Form)** which should be completed by the person amending the questionnaire when the subject is unable to personally make the changes. Any changes or additions must be consistent with subject's wishes and intent. OPM has a list of critical items on the three investigative forms that must be amended only by the subject.

B. Special Agreement Checks (SAC)

OPM can establish SACs with HHS to conduct specific records checks on individuals who need them to meet higher sensitivity levels. For example, to meet the NACIC requirement if an individual is moving from a Non-Sensitive (Level 1) position to a moderate risk Public Trust (Level 5), a credit record check only can be requested.

The SAC will consist of record checks only and requests for SAC agreements must be discussed with and approved by the Director, SDD.

C. Waivers

Special circumstances may require immediate action to employ an applicant or move an employee into a position designated as sensitive National Security (Level 3) or high risk Public Trust (Level 6). The situation may not permit sufficient time to complete the required preappointment investigation so a request for a waiver of that requirement may be made. (Waiver of the preappointment

investigation is not permitted for Level 4 positions since they are usually Presidential appointee positions which require an FBI investigation prior to the Senate confirmation process.)

1. When the head of an OPDIV or STAFFDIV, or a designated key official believes an emergency exists, that official shall submit a written waiver request (see example Exhibit A) to the Director, SDD. An original or automated SF 52 (Request for Personnel Action) must be included with the waiver for Non-career SES and Schedule C appointees. For all other employees, submit a copy of the original SF 52.

   Position sensitivity level 3 or 6 must be indicated in item 25 of the SF 52. Omission of information will delay final action on the request.

2. A waiver request must contain a brief statement of the reasons which constitute the conditions of the "emergency" as they relate to the national interest, and a statement that the nature of the "emergency" precludes the opportunity for a delay to conduct the required preemployment investigation.

3. All security forms for the required investigation must be submitted with the waiver request. If extenuating circumstances prevent this, the forms must be expeditiously forwarded to the Director, SDD, so that the investigation can be initiated within 14 days of placement. However, a current completed SF 86 or 85P is an investigative tool used in the waiver approval process and must be received and reviewed before the waiver is presented for approval. The waiver request action should be coordinated by the PSR.

4. For each waiver request, name checks are made to OPM and the FBI or other sources by SDD or designated officials. If checks and review of the SF 86/85P are favorable, the waiver will be approved and the original will be returned for placement in the employee's OPF. If other than favorable information is developed during the

waiver process, the waiver request may be disapproved and a preappointment investigation may be requested.

5. A waiver is not required for a Level 2 or 5 positions (except for non-career SES and Schedule C appointments), but a preappointment investigation is an option.

Security Clearances for Access to Classified Information

Whenever an employee or contractor requires access to classified national security information, the individual must be granted a security clearance at the proper level to access that information. The three security clearance levels are: Confidential, Secret, and Top Secret. The individual should request the clearance through his or her supervisor who must coordinate the request with the PSR. The Request for Security Clearance, HHS 207 form, must be completed and signed by the employee/contractor, the supervisor/recommending official, and the PSR. The HHS 207 should be forwarded to the Director, SDD, along with any forms needed for any required investigation.

A prerequisite to certification for access to classified information is completion of a favorable background investigation. The standard government-wide background investigation required for access to the various levels of classified information is as follows:

Confidential
or **Secret** - Access NACI **(ANACI)**

Top Secret - Single Scope Background Investigation **(SSBI)**

[Note: These are new OPM investigations developed because the President approved uniform investigative standards in March 1997 for Federal departments and agencies to use prior to granting the various security clearances.]

The Director, SDD, adjudicates the completed background investigation and determines whether to grant the requested security clearance. The Director, SDD, grants the clearance by signing the HHS 207 and forwarding a copy to the PSR who requested the clearance action. The PSR assures that the individual is briefed about security requirements. The signed original clearance certificate (HHS 207) is maintained in the official security file at SDD.

An interim security clearance can be granted to an individual for temporary eligibility for access to classified information prior to the completion and adjudication of the appropriate investigation. If there is a justifiable need for an interim clearance, the PSR or other requesting official must notify the Director, SDD, who will assure that the minimum investigative standards are met prior to granting the clearance. Note that the interim clearance can be revoked at any time based on unfavorable information identified in the course of the investigation.

Security Briefings

PSRs must assure that each employee and contractor who has been granted a security clearance receives briefings on security matters. Briefers should be familiar with the HHS National Security Information Manual and use it as a reference guide.

A. Initial security briefings must be conducted to inform individuals of the inherent responsibilities and proper procedures for handling and safeguarding classified information. This briefing must occur prior to the individual being given access to such information. During the briefing the individual should be given the security education briefing materials furnished by the Director, SDD.

   At the completion of initial security briefing, the employee or contractor is required to sign a Classified Information Nondisclosure Agreement (SF 312) and it shall be forwarded to the Director, SDD, for retention.

B. Refresher briefings must be given on a regular basis by PSRs to all individuals who have security clearances. They must be briefed on their continuing responsibilities for safeguarding classified information and on any new security regulations or procedures. Refresher briefings may be in oral, written, or electronic format. PSRs must maintain records to show that this requirement was met.

C. Security debriefings must be given to all individuals upon termination of their security clearances. They shall be advised of their continuing responsibility for

protecting the classified information to which they had access. Upon completion of the debriefing, the formerly-cleared individual must sign the bottom half of the SF 312 labeled "Security Debriefing Acknowledgment" and a witness also signs it. The SF 312 must be forwarded to the Director, SDD, for retention.

Clearance Terminations, Downgrades, and Denials

A PSR in coordination with the immediate supervisor and the Director, SDD, may determine a currently cleared individual no longer has a need for a security clearance. That determination is a discretionary one and the decision of the Director, SDD, is conclusive. Upon written notice to the individual, the PSR may administratively terminate, or downgrade, the security clearance in the following manner:

A. When it has been determined that a cleared individual no longer requires access to classified information, the security clearance must be administratively withdrawn by the appropriate PSR. The lower portion of the SF 312 must be completed and signed by the formerly-cleared individual and a witness. The PSR should annotate it to show that the action was administrative and without prejudice to the individual's future eligibility for access to classified information. The individual should be given a copy of the SF 312. The original must be immediately forwarded to the Director, SDD.

B. When the individual no longer requires access to a particular security clearance level, the PSR must annotate the new lower level on a copy of the current HHS Form 207 or prepare a new one showing the new requested level. This downgrading action on the HHS Form 207 must be dated and signed by the appropriate PSR and immediately forwarded to the Director, SDD, with a copy going to the subject.

Individuals who are being denied a security clearance, or having their clearance revoked, because they do not meet access eligibility standards must be given specific appeal rights as stipulated in EO 12968, Section 5.2, Review Proceedings for Denials or Revocation of Eligibility for Access. The Director, SDD, will coordinate the appeal process.

Reinvestigation Requirements

A. The incumbents of all positions for which access to Top Secret information has been granted must be subject to a SSBI-Periodic Reinvestigation (SSBI-PR) every five (5) years after the initial SSBI.

B. Incumbents of all positions for which access to Secret information has been granted must be subject to a NACLC every ten (10) years after the initial investigation.

C. The NACLC reinvestigation requirement for those with Confidential clearances is every fifteen (15) years.

The chart below shows the sensitivity/clearance level and the required reinvestigation:

Position Sensitivity/ Security Clearance Level	Reinvestigation Requirement
Levels 3 and 4 with **Top Secret** clearance	**SSBI-PR (every 5 years)**
Level 2 with **Secret** clearance	**NACLC (every 10 years)**
Level 2 with **Confidential** clearance	**NACLC (every 15 years)**

Requests for reinvestigations are forwarded to the Director, SDD, and consist of:

(1) Original and one copy of incumbent's current SF 86.

(2) Fingerprint chart (SF 87; or FD 258 if contractor) only when requested by SDD due to previously unclassifiable prints.

A more extensive investigation than the required one may be requested and scheduled when justified.

Safeguarding and Handling Investigative Reports

Personnel investigative reports and records must be safeguarded with the highest degree of discretion to protect the interests of

the individual and the Department. Therefore there are strict requirements for the control of investigative information and they are contained in HHS Personnel Instruction 731-1. Listed below are additional procedures:

A. All HHS officials, including PSRs, who review or store investigative reports and related information must have had a favorable determination based upon a background investigation that meets their sensitivity level. (Note: the minimum sensitivity level for those with these duties is Level 5, making this a moderate public trust position requiring the incumbent to be subject to a NACIC investigation.)

B. Copies of investigation reports, in whole or in part, must be controlled, safeguarded, and destroyed when the intended purpose has been served.

C. When personnel security/suitability investigation reports, including arrest records, and related adjudication materials are transmitted by mail, the addressee on the envelope must be the designated HHS official. Additionally, the envelope must bear the notation: *TO BE OPENED BY ADDRESSEE ONLY*.

D. When not in use, personnel security investigations and related adjudication materials must be stored in a combination-locked cabinet or safe or in an equally secure area.

E. Access to the container/area must be limited to authorized HHS officials, but they must not have access to their own investigative files.

F. All reports of investigation must be adjudicated within 90 days after receipt by the PSR.

G. All copies of investigation reports (including vouchers) received by the PSR or SPO must be destroyed within 60 days after the date of a favorable adjudication and must never be filed in the employee's OPF or forwarded to a contractor.

H. In cases involving a proposed adverse action, the investigation reports may be destroyed within 60 days after the action is complete, or forwarded to SDD for requested further retention.

EXHIBIT A

WAIVER EXAMPLE

MEMORANDUM TO: Doug Pruett
Director, Personnel Security
and Drug Testing Division, ASMB

FROM: Management Official
OPDIV/STAFFDIV

SUBJECT: Waiver of Preappointment Investigation on
Ima Niceguy

Executive Order 10450 provides that in case of emergency a person may be appointed to a sensitive position for a limited period prior to completion of a background investigation if such action is necessary in the national interest.

To insure that agency objectives and activities are continued without undue interruption, I am requesting a waiver of the preappointment investigation requirement on Ima Niceguy.

Mr. Niceguy has been selected for the position of Special Assistant to the Assistant Secretary. The expeditious filling of this position is critical to our mission.

Ima Niceguy will be responsible for a wide range of activities, including handling questions of a sensitive policy nature. Access to classified national security information is not required at this time and will be denied, unless subsequently a request for a security clearance is requested and approved.

Accordingly, I request your concurrence that an emergency situation exists and it is in the national interest to waive the preappointment investigation requirement.

Approved_____ Date_____
Authorizing Official

Attachments:

SF 85P or SF 86
SF 87
Resume

EXHIBIT B

INVESTIGATION SCHEDULING CHART

Leve1 1 (Non-Sensitive): use SF 85 to schedule NACI or CNACI

-SPO sends to OPM
-use OPDIV's SOI code (or SPO's, if assigned one)

Level 5 (Public Trust): use SF 85P to schedule NACIC

-OPDIV PSR sends to OPM
-use OPDIV's SOI code

Level 6 (Public Trust) use SF 85P to schedule BI

(and **Level 5** with increased to schedule LBI or MBI
risk & enhanced investigation)

-OPDIV PSR sends to SDD
-use SOI code: HE00

Level 2 (National Security) use SF 86 to schedule ANACI
Level 3 & 4 to schedule SSBI

-OPDIV PSR sends to SDD
-use SOI code: HE00