	U·S·DEPARTMENT OF THE INTERIOR **OFFICE OF SURFACE MINING** **RECLAMATION AND ENFORCEMENT** **DIRECTIVES SYSTEM**	**Subject Number:** PER-13 **Transmittal Number:** 278 **Date:** 10/14/86

Subject: PERSONNEL SECURITY PROGRAM

Approval: Jed D. Christensen **Title:** Director

1. Purpose. This directive establishes the policy and procedure for determining position sensitivity and investigative requirements and the rules for handling and safeguarding classified national security information as applied to the Office of Surface Mining Reclamation and Enforcement. In addition, this directive supplements and implements Executive Order 10450, Security Requirements for Government Employment; Executive Order 12356 and Information Security Oversight Office, Directive No. 1, on National Security Information; Office of Management and Budget, Circular A-71, Security of Federal Automated Information Systems; Federal Personnel Manual (FPM) Chapter 732, Personnel Security; 441 Departmental Manual (DM) Chapters 1-8, Clearances and Suitability Investigative Requirements; and, 442 Departmental Manual (DM) Chapters 1-15, National Security Information.

2. Definitions.

a. Access, Accessibility. The ability and opportunity to obtain knowledge of classified information. An individual may be considered to have access just by being in a place where the information is used or stored if sufficient security measures are not taken to prevent gaining knowlege of the information. (ref.: 441 DM 2.1)

b. Automatic Data Processing (ADP) Security. Security concerned with data integrity and protection of information resources from modification, loss, or destruction. (ref.: 441 DM 2.1)

c. Authorized Persons. Persons who have a need-to-know and have been cleared for the receipt of the information. Responsibility for determining whether an individual's duties require access to classified information and is authorized to receive it, rests with the individual who has possession, knowledge, or control of the information not with the recipient. (ref.: 441 DM 2.1)

d. Classified Information. Official information which has been identified and marked as TOP SECRET, SECRET, or CONFIDENTIAL in the interest of national security. (ref.: 441 DM 2.1)

e. Clearance (Security). An administrative determination based upon the results of an investigation that an individual is trustworthy and may be granted access to classified information as required in the performance of assigned duties. (441 DM 2.1)

f. Confidential. Refers to that national security information or material, the unauthorized disclosure of which could reasonably be expected to cause damage to the national security. (ref.: 442 DM 2.1)

g. Industrial Security. The area of internal security which is concerned with the protection of classified information in the hands of United States industry. (ref.: 442 DM 2.1)

h. National Security Information. Data determined to require protection and preservation of the military, economic and productive strength of the United States, including the security of the Government in domestic and foreign affairs, against or from espionage, sabotage and subversion, and any and all other illegal acts designed to weaken or destroy the United States. (ref.: 441 DM 2.1)

i. Need-To-Know. In addition to a security clearance, an individual must have a need for access to the classified information or material sought in connection with the performance of assigned official duties or contractual obligations. The determination as to whether access will be granted lies with the officials(s) having responsibility for the classified information or material. (ref.: 442 DM 2.1)

j. Physical Security. Physical safeguards designed for the protection and welfare of personnel, facilities, equipment, and material. These safeguards would include guard service, alarm systems, visitor control, etc. (ref.: 442 DM 2.1)

k. Secret. Refers to that national security information or material, the unauthorized disclosure of which could reasonably be expected to cause serious damage to the national security. (ref.: 442 DM 2.1)

l. Security. Safeguarding of information classified TOP SECRET, SECRET, or CONFIDENTIAL against unlawful or unauthorized dissemination, duplication, or observation. (ref.: 442 DM 2.1)

m. Security Folder. A file of completed security documents not prescribed for inclusion in the employee's official personnel folder. These folders are maintained by the security office and access thereto is in conformance with Freedom of Information and Privacy Acts. (ref.: 441 DM 2.1)

n. Top Secret. Refers to that national security information or material, the unauthorized disclosure of which could reasonably be expected to cause exceptionally grave damage to the national security. (ref.: 442 DM 2.1)

o. Unauthorized Person. Any person not authorized to have access to specific classified information. Regardless of the degree of clearance, an individual is not authorized access to classified information of any degree without a demonstrated need-to-know. (ref.: 442 DM 2.1)

3. Policy/Procedures.

a. Security clearances will only be obtained for those employees whose current position requires one as a condition of effective job performance.

b. Responsibilities. (ref.: 441 & 442 DM)

(1) The Director, Office of Surface Mining Reclamation and Enforcement, has the responsibility for implementing and administering a security clearance program wherein classified information and materials are safeguarded and in conformance with governing policies, rules, and regulations. He/she may designate appropriately cleared personnel to assist in the discharge of these responsibilities. The following identifications have been made:

(a) The Assistant Director, Budget and Administration has been designated as the Security Officer to ensure the integrity of classified information and material under his/her jurisdiction and to assist the Director in the discharge of security responsibilities.

(b) The Personnel Officer has been designated as the Alternate Security Officer to ensure the integrity of classified information and material under his/her jurisdiction and to assist the Security Officer in the discharge of security responsibilities.

1 The Administrative Service Center Chiefs and the Administrative Officers have been designated to assist the Alternate Security Officer in the procedural aspects of the Program for field personnel. A list of individuals having security records on file with the Alternate Security Officer will be sent to the appropriate support office.

These duties include, but are not limited to obtaining and submitting to the Alternate Security Officer the following:

a Personnel Security Action Requests and related investigative paperwork.

b ADP Access Terminations.

c Security Termination Statements (except Top Secret).

(c) A staff member from the Information Systems Management Staff has been designated as the ADP Security Officer to ensure the integrity of classified information and material under his/her jurisdiction and to assist the Director in the discharge of security responsibilities.

(d) Officials have the responsibility for the security of classified information to the same degree as for the functional responsibility of the organizational unit.

(e) Individuals have a basic responsibility for the integrity and security of classified information in their possession or knowledge.

b. Procedures.

(1) How to Determine Position Sensitivity. In coordination with the Branch of Personnel Services and the Administrative Service Centers, officials have the responsibility for ensuring that position sensitivity is properly identified and recorded on the OF-8, SF-50, and SF-52 for all positions in the Agency. Also, in coordination with the ADP Security Officer, they have the responsibility for determining the ADP access requirements for positions under their jurisdiction in accordance with expressed ADP guidelines.

(a) General Definitions of Sensitivity Levels.

1 Special-Sensitive Level 4. Includes any position determined to be in a level higher than Critical-Sensitive because of (1) the greater degree of damage that an individual by virtue of occupancy of the position could effect to the national security, (2) special requirements concerning the position under any authority other than E.O. 10450 or, (3) a risk imposed in terms of ADP-Computer security above that at the Critical-Sensitive level.

2 Critical-Sensitive Level 3. Includes positions involving any of the following:

a Access to Top Secret defense information;

b Development or approval of war plans, plans or particulars of future or major or special operations of war, or critical and extremely important items of war;

c Development or approval of plans, policies or programs which affect the overall operations of an agency; that is, policy-making or policy-determining positions;

d Investigative duties, the issuance of personnel security clearances, or duty on personnel security boards; or

e Fiduciary, public contact, or other duties demanding the highest degree of public trust.

Also, includes positions in which the incumbent is responsible for the planning, direction and implementation of a computer security program; has a major responsibility for the direction, planning, and design of a computer system, including the hardware and software; or, can access a system during the operation or maintenance in such a way, that provides a relatively high risk for causing grave damage or realizing significant personal gain. Such positions may involve:

- Responsibility for the development and administration of agency computer security programs, and also including direction and control of risk analysis and/or threat assessment.

- Significant involvement in life-critical or mission-critical systems.

- Responsibility for the preparation or approval of data for input into a system which does not necessarily involve personal access to the system, but with relatively high risk for effecting grave damage or realizing significant personal gain.

- Relatively high risk assignments associated with or directly involving the accounting, disbursement, or authorization for disbursement from systems of (1) dollar amounts of $10 million per year or greater, or (2) lesser amounts if the activities of the individual are not subject to technical review by higher authority at the Critical-Sensitive level to insure the integrity of the system.

- Positions involving major responsibility for the direction, planning, design, testing, maintenance, operation, monitoring, and/or management of systems hardware and software.

- Other positions as designated that involve relatively high risk for effecting grave damage or realizing significant personal gain.

3 Noncritical-Sensitive Level 2.
Includes positions that involve one of the following:

a Access to Secret or Confidential national security materials, information, etc.

b Duties that may directly or indirectly adversely affect the overall operations of the agency.

c Duties that demand a high degree of confidence and trust.

Also, include positions in which the incumbent is responsible for the direction, planning, design, operation, or maintenance of a computer system, and whose work is technically reviewed by a higher authority at the Critical-Sensitive level to insure the integrity of the system. Such positions may involve:

- Responsibility for system design, operation, testing, maintenance, and/or monitoring that is carried out under technical review of higher authority at the Critical-Sensitive level, to insure the integrity of the system. This level includes, but is not limited to:

. access to and/or processing of proprietary data, information requiring protection under the Privacy Act of 1974, and Government-developed privileged information involving the award of contracts;

. accounting, disbursement, or authorization for disbursement from systems of dollar amounts less than $10 million per year.

- Other positions as designated that involve a degree of access to a system that creates a significant potential for damage or personal gain less than that in Critical-Sensitive positions.

4 Non-Sensitive Level 1. Includes all positions not falling into one of the above sensitive levels.

Also, includes all ADP-computer positions not falling into one of the above sensitive levels.

(b) Coding of Position Sensitivity on Personnel Documents.

Sensitivity Level	Coding*
Special-Sensitive	4
Critical-Sensitive	3
Noncritical-Sensitive	2
Non-Sensitive	1

*ADP-Computer positions will be identified by the letter "C" after the above coding.

(2) How to Request Personnel Security Action. Once the responsible official has made the decision on the position sensitivity/access, the following documentation must be transmitted to the Alternate Security Officer prior to the appointment or transfer of an employee into a sensitive position:

(a) One copy of SF-52 for new employees. A memorandum is acceptable to effect the amendment on the OF-8, SF-50, and SF-52 for current employees.

(b) One copy of Personnel Security Action Request, Form DI 1913. (See Illustration 1) Part I is to be completed by the originating office. Part II is to be completed by the Division of Personnel.

(c) A waiver request, Form DI 1912, (See Illustration 2), in emergency situations if a noncritical/critical-sensitive position must be filled by an individual for whom the appropriate investigation has not been completed. The originating office should provide enough pertinent information to allow the Alternate Security Officer to complete the remainder of the form. (ref.: 441 DM 5.1)

Upon completion of the investigation, a notice will be sent to the requesting official and a copy placed in the employee's official personnel folder, specifying the type of investigation, who conducted the investigation, and the date of completion. (See Illustration 3)

(3) Prior Investigations by Other Federal Government Agencies. A prior investigation by any agency of the Federal Government may meet the investigative requirements of a position, however, this determination will be made by the Alternate Security Officer. (ref.: 441 DM 5.2)

(4) Prior Security Clearance. Prior security clearances issued by other Government agencies automatically terminate when an employee transfers to another Department. (ref.: 441 DM 5.3)

(5) Intra-Departmental Transfers. When a cleared employee transfers within the Department of the Interior, the security file will be transferred to the receiving Security Office where it can be used as the basis for satisfying suitability and/or clearance requirements. (ref.: 441 DM 5.4)

(6) When and How to Cancel Investigations. The Alternate Security Officer should be notified immediately if the subject of an investigation resigns, terminates, or otherwise is no longer being considered for a clearance in order that appropriate action may be taken regarding the requested investigation. (ref.: 441 DM 5.9)

c. Investigative Costs. The cost of investigations other than for entry level NAC/NACI's are borne by the requesting office. (FPM 736, 2-11) Cost for investigation of contractor employees will be borne by the contracting activity. However, contracting officials should assure that the requirements are clearly defined in the contractural document to prevent resistance by contract employees in filling out the necessary investigative paperwork. (ref.: 441 DM 6.8 & 6.11)

A copy of the current Office of Personnel Management billing rates for investigative services has been included for budgeting purposes. (See Illustration 4).

d. Briefings/Debriefings, Certifications, and Terminations.

(1) Security Briefing/Debriefing. All presently cleared personnel and newly cleared employees prior to initial access to classified information, will be briefed by the Alternate Security Officer on the contents of Part 442 DM. Following the briefing, the individual will be required to complete the Classified Information Nondisclosure Agreement, Form SF-189, as a prerequisite to access, and will receive a copy of the directive. (See Illustration 5) (ref.: 442 DM 4.2)

A Security Termination Statement will be obtained by the appropriate designated responsible official, at the time an employee terminates, is reassigned, or when clearance is withdrawn for any reason. This debriefing, which is the explanation of the form, will be accomplished in the presence of a witness. When the employee has access to TOP SECRET information, an oral debriefing will be administered by the Alternate Security Officer. (See Illustration 6) (ref.: 442 DM 4.3)

(2) Foreign Travel Briefing/Debriefing. Foreign Travel Certification (Form DI 1175) will be processed through the Department Security Office by the Office of the Assistant Secretary--Territorial and International Affairs prior to approval when travel involves Communist countries or participants. This provision exists regardless of whether a security clearance is a requirement for the proposed travel. These forms should be sent to the Alternate Security Officer for routing.

All employees traveling to Communist controlled countries or to attend meetings where representatives of Communist countries will attend must be briefed by the Alternate Security Officer. (See Illustration 6, Part I) This provision includes travel for official and personal reasons. Employees traveling on personal business should contact the Alternate Security Officer at least 10 days prior to departure to arrange for a briefing. Upon return from travel, required debriefings will be accomplished by the Alternate Security Officer to determine whether the employee was subject to any hostile intelligence efforts. (See Illustration 7, Part II)

Communist countries are: Albania, Bulgaria, Cambodia, People's Republic of China (Communist China, including Tibet), Cuba, Czechoslovakia, Communist Korea (North Korea), German Democratic Republic (German Democratic Republic-East Germany, including the Soviet Sector of Berlin), Hungary, Laos, Mongolian People's Republic (Outer Mongolia), Poland, Rumania, Union of Soviet Socialist Republics (U.S.S.R., including Estonia, Latvia, Lithuania, Kurile Islands and South Sakhalin (Karafuto), and all other constituent Republics), Vietnam, and Yugoslavia. (ref.: 442 DM 4.4)

(3) Certifications. Clearances are granted only in cases where originating office specifies that access to classified material will be required in the performance of the incumbent's duties. In such cases, the Alternate Security Officer will issue a Certificate of Clearance, DI 1916, upon receipt of a favorable investigation. (See Illustration 8) (ref.: 441 DM 7.4)

In cases where access to classified material is not required for sensitive positions, the Alternate Security Officer will issue a Certification of Favorable Determination for a Noncritical/Critical Sensitive Position, DI 1917. (See Illustration 9) (ref.: 441 DM 7.4)

Before an employee assumes the duties of a noncritical or critical sensitive position for which a clearance is not required, he/she must be briefed by the appointing official regarding the sensitivity and inherent responsibilities of the position. A briefing statement will be completed and sent to the Alternate Security Officer for inclusion in the employee's security folder. (See Illustration 10) (ref.: 441 DM 7.6)

ADP positions not requiring access to classified information will receive a certification of ADP access. (See Illustration 11) (ref.: 441 DM 7.4)

(4) ADP Access Termination. An ADP Access Termination Statement, DI-1915, will be obtained by the appropriate designated responsible official, at the time an employee terminates employment; transfers to a position wherein ADP access is not required; departs on leave of absence in excess of one year; or transfers to another agency. (See Illustration 12) (ref.: 441 DM 6.9)

e. Maintenance and Disposal of Security Records. Security folders will contain a copy of every action affecting the status of an individual's security clearance or suitability adjudication. The minimum documentation maintained will be as follows (ref.: 441 DM 5.8):

(1) SF-52 showing designation of position sensitivity.

(2) A completed copy of Form DI 1913 and 1912, if appropriate.

(3) Copies of all personal history forms with the expection of the SF-87, Fingerprint Card.

(4) Copy of OPM Form 1474, Agency Request for Reimbursable OPM Personnel Investigation.

(5) Stamped copies of the SF-85 and SF-171 for Noncritical-Sensitive Positions or OPI 79A, Agency Adjudicative Action of Personnel Investigations Material after investigations have been processed.

(6) Signed SF-189 for individuals possessing security clearances.

(7) A copy of the ADP Access Authorization.

Security records maintained by the Security Office will be disposed of in accordance with Schedule 18 of the General Records Schedule, as follows:

Personnel security clearance case files and related indices will be destroyed upon notification of death or not later than five years after separation, termination, or expiration of contract relationship.

Lists or rosters showing current security clearance status of individuals will be destroyed when superseded or obsolete.

4. Reporting Requirements. As specified in the Federal Personnel Manual and the Departmental Manual.

5. References. Relevant sections of the Federal Personnel Manual, Departmental Manual, and General Records Schedules.

6. Effect on Other Documents. Supersedes PER 13, Transmittal No. 229, dated August 8, 1984.

7. Effective Date. Upon issuance.

8. Contact. Alternate Security Officer, (202) or FTS 343-4665.

U.S. DEPARTMENT OF THE INTERIOR
PERSONNEL SECURITY ACTION REQUEST

PART I - ORIGINATING OFFICE

Candidate's Name	Date of Birth	Place of Birth
Position Title and Grade	E.O.D. Date	Account Number
Bureau/Office	Duty Location	Status (Check One) ☐ Applicant ☐ Employee

POSITION SENSITIVITY/ACCESS REQUIREMENTS:

CRITICAL-SENSITIVE (Check Appropriate Block(s))

- ☐ Access to TOP SECRET national security information and/or sensitive compartmented information.
- ☐ Investigative and/or supervisory law enforcement duties, security officers, and/or personnel security specialists.
- ☐ Fiduciary, public contact, or other duties demanding a high degree of public trust.
- ☐ Foreign assignments in excess of 130 days.
- ☐ Positions designated as ADP-I.*(See 441 DM 6, Appendix 1.)
- ☐ Implementing foreign policy objectives and/or protecting against foreign aggression.
- ☐ Protecting against internal subversion, espionage, sabotage, or other acts which threaten public safety or U.S. internal security.
- ☐ Participation in negotiations with foreign representatives on matters having international impact.
- ☐ Development or approval of plans, policies, or programs which affect the overall operations of an agency; that is policy making or policy-determining positions.
- ☐ Other, explain.

NONCRITICAL-SENSITIVE (Check Appropriate Block(s))

- ☐ Access to SECRET or CONFIDENTIAL national security information.
- ☐ A foreign assignment of 130 days or less duration.
- ☐ Mail room employees and messengers specifically designated to carry classified material.
- ☐ Non-supervisory law enforcement and/or non supervisory fiduciary positions.
- ☐ Positions designated as ADP-II.*
- ☐ Other, explain.

Date of Request	Requesting Office	Signature of Requesting Official

PART II - PERSONNEL OFFICE
To transmit investigative papers or information to personnel security office.

DATA ON PREVIOUS INVESTIGATION

- ☐ NACI Investigation. OPM Stamp on Employment Application ("X" One and Complete)
  - ☐ Processed Under Section 3(a) of E.O. 10450 — Date:
  - ☐ Results of Investigation under Section 3(a) of E.O. 10450 furnished Requesting Agency — Date:
- ☐ Full Field or Other Background Investigation (Specify)
  - Completed by: — Date:
- ☐ NO EVIDENCE OF INVESTIGATION - Request for Waiver Attached
- ☐ Other Investigative/Clearance Information:

PAPERS SUBMITTED FOR NEW INVESTIGATION

- ☐ None. No break in service of over one year since prior investigation. SF 171 or Personal History Statement attached.
- ☐ PAPERS FOR BACKGROUND INVESTIGATION ATTACHED (Three SF 86, one SF 87, OPM Document 14, OPM 329, 329 A, B, and C.)
- ☐ PAPERS FOR NONCRITICAL-SENSITIVE NACI ATTACHED. (SF 85 set, SF 87, OPM Document 14, two SF-171.)
- ☐ OTHER ATTACHMENTS (List)

DATE	PERSONNEL OFFICE	SIGNATURE OF PERSONNEL OFFICIAL

*NOTE: EFFECTIVE 1/6/84 ADP I = 3 AND ADP II = 2.

DI 1913
(5/83)

Guidelines for Designating ADP Categories for Positions Associated with Federal Computer Systems

This document provides specific criteria and amplifying guidance for determining the category of each position associated with Department computer systems.

Criteria for Designating Positions

Three categories have been established for designating computer and computer-related positions -- ADP-I, ADP-II, and ADP-III. Specific criteria for assigning positions to one of these categories are as follows:

Category	Criteria
~~ADP-I~~ ADP 3 (eff.: 1/6/84)	- Responsibility for the development and administration of agency computer security programs, and also including direction and control of risk analysis and/or threat assessment.
	- Significant involvement in life-critical or mission-critical systems.
	- Responsibility for the preparation or approval of data for input into a system which does not necessarily involve personal access to the system, but with relatively high risk for effecting grave damage or realizing significant personal gain.
	- Relatively high risk assignments associated with or directly involving the accounting, disbursement, or authorization for disbursement from systems of (1) dollar amounts of $10 million per year or greater, or (2) lesser amounts if the activities of the individuals are not subject to technical review by higher authority in the ADP-I category to ensure the integrity of the system.
	- Positions involving major responsibility for the direction, planning, design, testing, maintenance, operation, monitoring, and/or management of systems hardware and software.
	- Other positions as designated by the agency head that involve relatively high risk for effecting grave damage or realizing significant personal gain.

~~ADP-II~~
ADP 2
(eff.: 1/6/84) - Responsibility for systems design, operation, testing, maintenance, and/or monitoring that is carried out under technical review of higher authority in the ADP-I category, to ensure the integrity of the system. This category includes, but is not limited to:

(1) access to and/or processing of proprietary data, information requiring protection under the Privacy Act of 1974, and Government-developed privileged information involving the award of contracts;

(2) accounting, disbursement, or authorization for disbursement from systems of dollar amounts less than $10 million per year.

- Other positions as designated by the agency head that involve a degree of access to a system that creates a significant potential for damage or personal gain less than that in ADP-I positions.

~~ADP-III~~
ADP 1 (eff.: 1/6/84) - All other positions involved in Federal computer activities.

Guidelines for Applying Criteria to Specific Positions

In determining category levels for Federal computer positions, heads of bureaus and offices should consider not only the specific requirements of the position but also the relationship of those requirements to the informational system that the position services. For example, information that is not in itself highly sensitive may in combination with similar, low sensitive data, produce a highly sensitive system. A position, which involves limited access to and use of selected systems data for specific purposes during limited periods of time in a controlled situation, may be considered for a lower ADP category. Such positions might have less potential for harm than a position associated with the system's design, operation or maintenance involving access to or control of large amounts of data in the system which, in combination, may be extremely critical to life or mission.

Application of the criteria for designating category levels of individual positions normally does not fit a precise formula. A determination must be made on the basis of judgment, considering numerous factors, including, but not necessarily limited to:

- the degree of supervision or review afforded the occupant of the position;

- the extent of security and protective measures in effect;

- the nature of the data being processed;

- the degree to which the data being processed is accessible by the individual through outside terminals;

- the extent to which responsibility for violations or attempted violation of computer systems security can be established;

- the extent to which the activities associated with the position are performed in isolation from concurrent processes; and

- the degree of accessibility to other data in a system through intrusion by telecommunications or time sharing.

Based upon these and other considerations, agencies should define determinants such as "significant involvement," "grave damage," and "significant personal gain" in terms of the individual bureau or office mission and the relative risks associated with the particular system or systems involved. On a continuing basis, an assessment of all category designations should be made to identify any changes in the data available or the duties and responsibilities of the position that would cause the position to be placed in a higher or lower category level.

Screening Persons for Assignment to ADP-I, ADP-II, and ADP-III Positions

Heads of bureaus and offices are responsible for developing criteria for screening persons for assignment to ADP-I, ADP-II, and ADP-III positions. Office of Personnel Management suitability guidelines in Federal Personnel Manual Supplement 731-1 and the guidelines in Executive Order 10450 may be used in developing this criteria. Bureaus and offices should also consider any other factors which have a bearing on the person's trustworthiness. Individual agency criteria for Federal civilian competitive service positions may also be used for any other personnel associated with Federal computer systems.

UNITED STATES
DEPARTMENT OF THE INTERIOR

ILLUSTRATION 2

Memorandum

To: Departmental Security Officer

Through: Bureau Personnel Officer

From: Head of Bureau or Office

Subject: Request for Waiver of Preappointment Investigative Requirements

In accordance with the provisions of section 3b of Executive Order 10450, it is requested that preappointment investigative requirements be waived for the following individual:

Name: _____
Organization: _____
Current DOI Security Clearance: _____
Proposed Position Title: _____
Immediate Supervisor: _____
Proposed EOD (date): _____

A waiver of preappointment investigative requirements is necessary because:

_____
_____
_____

If approved, I will ensure that the individual will not have access to any classified information prior to the granting of a security clearance, or will have access only to the level of his/her current DOI clearance. Forms required for the investigation were submitted to _____ (Security Officer) on _____ (Date).

I certify that this request is urgent, is in the national interest, and recommend approval.

_____ (Head of Bureau or Office) _____ (Date)

Based on my review of the individual's previous employment record and knowledge of this candidate's background, there appears to be no derogatory information which would preclude employment in a sensitive position pending completion of the required investigation.

_____ (Bureau Personnel Officer) _____ (Date)

RECOMMEND APPROVAL: _____ (Department Security Officer) _____ (Date)

APPROVED: _____
Assistant Secretary - Policy, Budget and Administration _____ (Date)

Original: Employee's OPF
cc: Employee's Security File
Appropriate Headquarter's Official
Director of Personnel
Departmental Security Officer

DI-1912
(5/83)

United States Department of the Interior

OFFICE OF SURFACE MINING
Reclamation and Enforcement
WASHINGTON, D.C. 20240

Memorandum

To:

From: Alternate Security Officer

Subject: Security Notice

This is to advise that subject has been favorably processed under E.O. 10450, _____ conducted by the _____ and the appropriate security clearance has been granted. Subject's security folder with all supporting documents is maintained by this office.

This notice will be placed in the Official Personnel File of _____. Upon change in his/her employment status, i.e., resignation, transfer to another department, etc., please contact this office so that the necessary paperwork can be processed.

If further information is needed, please telephone me or Peggy Moran, Program Specialist, on (202) or FTS 343-4665.

Ann L. Chapman

ILLUSTRATION 4
Attachment to FPM Bulletin 736-13

BILLING RATES EFFECTIVE 8/1/86

Type of Investigation	35 Days Service	75 Days Service	120 Day Service
CS - (Credit Search)	$ 6	-	-
NAC - (National Agency Check)	$ 8	-	-
NAC&C - (National Agency Check & Credit)	$ 14	-	-
NACI - (National Agency Check & Inquiries) (35 Days/Sensitive & 75 Days/Non-Sens)	$ 14	$ 14	-
NACIC - (National Agency Check, Inquiries, and Credit) (35 Days/Sens & 75 Days/Non-Sen)	$ 20	$ 20	-
PRI - (Periodic Reinvestigation)	-	-	$ 75
MBI - (Minimum Background Investigation)	-	-	$ 100
UDI - (Update Investigation) 13-36 months	-	-	$ 50
UDI - (Update Investigation) 37-60 months	-	-	$ 75
RSI - (Reimbursable Suitability Investigation)	-	-	$ 400
LBI - (Limited Background Investigation)	$1,100	$ 800	$ 650
UGI - UDI (Upgrade and Update Investigations)			
From 13-36 months	$ 550	$ 400	$ 325
From 37-60 months	$ 825	$ 600	$ 500
BI - (Background Investigation)	$1,900	$1,600	$1,450
UGI - UDI (Upgrade and Update Investigations)			
From 13-36 months	$ 950	$ 800	$ 725
From 37-60 months	$1,425	$1,200	$1,100
SBI - (Special Background Investigation)	$2,125	$1,825	$1,675
UGI - UDI (Upgrade and Update Investigations)			
From 13-36 months	$1,075	$ 925	$ 850
From 37-60 months	$1,600	$1,375	$1,250

Note: UGI are from level below (i.e., LBI from MBI, BI from LBI, SBI from BI). UGI and UDI are based on a percentage of basic case price (i.e., 50% from 13-36 months and 75% from 37-60 months)

*U.S. GOVERNMENT PRINTING OFFICE:1986-490-572:2539

CLASSIFIED INFORMATION NONDISCLOSURE AGREEMENT

An Agreement Between _____ and the United States
(Name - Printed or Typed)

1. Intending to be legally bound, I hereby accept the obligations contained in this Agreement in consideration of my being granted access to classified information. As used in this Agreement, classified information is information that is either classified or classifiable under the standards of Executive Order 12356, or under any other Executive order or statute that prohibits the unauthorized disclosure of information in the interest of national security. I understand and accept that by being granted access to classified information, special confidence and trust shall be placed in me by the United States Government.

2. I hereby acknowledge that I have received a security indoctrination concerning the nature and protection of classified information, including the procedures to be followed in ascertaining whether other persons to whom I contemplate disclosing this information have been approved for access to it, and that I understand these procedures.

3. I have been advised and am aware that direct or indirect unauthorized disclosure, unauthorized retention, or negligent handling of classified information by me could cause irreparable injury to the United States or could be used to advantage by a foreign nation. I hereby agree that I will never divulge such information unless I have officially verified that the recipient has been properly authorized by the United States Government to receive it or I have been given prior written notice of authorization from the United States Government Department or Agency (hereinafter Department or Agency) last granting me a security clearance that such disclosure is permitted. I further understand that I am obligated to comply with laws and regulations that prohibit the unauthorized disclosure of classified information.

4. I have been advised and am aware that any breach of this Agreement may result in the termination of any security clearances I hold; removal from any position of special confidence and trust requiring such clearances; and the termination of my employment or other relationships with the Departments or Agencies that granted my security clearance or clearances. In addition, I have been advised and am aware that any unauthorized disclosure of classified information by me may constitute a violation or violations of United States criminal laws, including the provisions of Sections 641, 793, 794, 798, and 952, Title 18, United States Code, the provisions of Section 783(b), Title 50, United States Code, and the provisions of the Intelligence Identities Protection Act of 1982. I recognize that nothing in this Agreement constitutes a waiver by the United States of the right to prosecute me for any statutory violation.

5. I hereby assign to the United States Government all royalties, remunerations, and emoluments that have resulted, will result or may result from any disclosure, publication, or revelation not consistent with the terms of this Agreement.

6. I understand that the United States Government may seek any remedy available to it to enforce this Agreement including, but not limited to, application for a court order prohibiting disclosure of information in breach of this Agreement.

7. I understand that all information to which I may obtain access by signing this Agreement is now and will forever remain the property of the United States Government. I do not now, nor will I ever, possess any right, interest, title, or claim whatsoever to such information. I agree that I shall return all materials which have, or may have, come into my possession or for which I am responsible because of such access, upon demand by an authorized representative of the United States Government or upon the conclusion of my employment or other relationship with the Department or Agency that last granted me a security clearance. If I do not return such materials upon request, I understand that this may be a violation of Section 793, Title 18, United States Code, a United States criminal law.

8. Unless and until I am released in writing by an authorized representative of the United States Government, I understand that all conditions and obligations imposed upon me by this Agreement apply during the time I am granted access to classified information, and at all times thereafter.

9. Each provision of this Agreement is severable. If a court should find any provision of this Agreement to be unenforceable, all other provisions of this Agreement shall remain in full force and effect.

10. I have read this Agreement carefully and my questions, if any, have been answered to my satisfaction. I acknowledge that the briefing officer has made available to me Sections 641, 793, 794, 798, and 952 of Title 18, United States Code, Section 783(b) of Title 50, United States Code, the Intelligence Identities Protection Act of 1982, and Executive Order 12356, so that I may read them at this time, if I so choose.

11. I make this Agreement without mental reservation or purpose of evasion.

SIGNATURE	DATE	SOCIAL SECURITY NO. *(See notice below)*

ORGANIZATION

The execution of this Agreement was witnessed by the undersigned, who, on behalf of the United States Government, agreed to its terms and accepted it as a prior condition of authorizing access to classified information.

WITNESS AND ACCEPTANCE:

SIGNATURE	DATE

ORGANIZATION

NOTICE: The Privacy Act, 5 U.S.C. 552a, requires that federal agencies inform individuals, at the time information is solicited from them, whether the disclosure is mandatory or voluntary, by what authority such information is solicited, and what uses will be made of the information. You are hereby advised that authority for soliciting your Social Security Account Number (SSN) is Executive Order 9397. Your SSN will be used to identify you precisely when it is necessary to 1) certify that you have access to the information indicated above or 2) determine that your access to the information indicated has terminated. Although disclosure of your SSN is not mandatory, your failure to do so may impede the processing of such certifications or determinations.

DEPARTMENT OF THE INTERIOR
SECURITY TERMINATION STATEMENT

TYPED OR PRINTED NAME	TYPE CLEARANCE	BUREAU/OFFICE

SOCIAL SECURITY NUMBER	DATE AND PLACE OF BIRTH

I am aware that the authorization for my access to classified information is hereby terminated. I am informed of my continuing responsibility for safeguarding the knowledge of classified information which I have gained during my employment. In fulfillment of this obligation, I certify that:

1. I do not have in my possession or control any document or material of a classified nature.

2. I will not knowingly or willfully divulge, reveal, or transmit classified information orally or in writing or by any other means, to any unauthorized person or agency.

3. I have read the provisions of the appropriate espionage laws, and other Federal statutes. I understand that any unauthorized disclosure of information affecting the national defense is prohibited and punishable by law.

4. I will report to the Federal Bureau of Investigation, to a Security Officer of the Department of the Interior, or to a Security Officer of a U.S. Embassy or Consulate, without delay, any incident wherein an attempt is made by an unauthorized person to solicit or obtain classified information.

5. I, have, have not (strike out inappropriate word or words) received an oral security debriefing.

SIGNATURE	DATE

TYPED OR PRINTED NAME OF DEBRIEFER	SIGNATURE OF DEBRIEFER

PRIVACY ACT NOTICE: In compliance with the Privacy Act of 1974, the following information is provided: Solicitation of the information requested on this form is authorized under Executive Order 12356. The purpose of this information is to confirm that the employee has received a security debriefing. Routine use of this information may be by Federal, State and local agencies when relevant to security investigations and/or violations. Refusal to provide the requested information may result in appropriate administrative action and/or unauthorized exit clearance.

DEPARTMENT OF THE INTERIOR
FOREIGN TRAVEL
DEFENSIVE SECURITY BRIEFING/DEBRIEFING STATEMENTS

PART I - SECURITY BRIEFING

Full Name of Traveler: _____
Date and Place of Birth: _____
Clearance Status: _____

Brief description of projects and classification of information to which access was provided during the past two years:

_____

_____

Countries to be visited and inclusive dates of travel: _____

_____

I certify that I have been given a defensive security briefing relative to my proposed travel to or through the above listed countries, and understand my responsibility for safeguarding information incident to my foreign travel.

_____ _____
(Signature of Traveler) (Signature of Security Officer)

Date: _____

PART II - DEBRIEFING STATEMENT

Date: _____

Narrative statement of the circumstances surrounding hostile intelligence efforts to obtain information or to compromise the traveler, or any endeavor to establish a continuing relationship. (If none, so state.)

_____

_____

_____

_____
(If necessary, continue on reverse side.)

_____ _____
(Signature of Traveler) (Signature of Debriefing Official)

PRIVACY ACT NOTICE: In compliance with the Privacy Act of 1974, the following information is provided: Solicitation of the information requested on this form is authorized under Executive Order 12356. The purpose of this information is to confirm that the employee has received a security briefing before foreign travel and debriefing after return from foreign travel. Routine use of this information may be by Federal, State and local agencies when relevant to security investigations and/or violations. Refusal to provide the requested information will result in denial of the requested travel authorization.

DI 1911 (June 83)

U.S. DEPARTMENT OF THE INTERIOR

Memorandum

To:

From:

Subject: Certification of Security Clearance of

NAME:
SSN:

This is to certify that a security clearance for access to classified information or material up to and including _____ has been granted, this date, to the above-named employee. The employee was briefed on his/her responsibilities in safeguarding classified documents, as specified in 442 DM 1-15.

This action was based on a favorable investigation conducted by an authorized investigative element of the U.S. Government. The information contained in their report indicates that the employment of this individual in a sensitive position is clearly consistent with the interests of national security as defined in E.O. 10450.

When access to classified information or material is no longer required, whether due to a "need to know" or termination of employment, this office must be notified in order to insure that the employee concerned completes a Security Termination Statement and that his/her clearance is terminated.

This notice of clearance is not to be furnished to the individual concerned, but is to be retained on file by his/her supervisor at the office of assignment.

U.S. DEPARTMENT OF THE INTERIOR

Memorandum

To:

From:

Subject: Certification of Favorable Determination for a Noncritical/Critical Sensitive Position

Name:
SSN:

Based on a favorable _____, conducted by _____ on _____, the appointment of the above-named individual to a noncritical/critical-sensitive position is clearly consistent with the interests of the national security as defined in Executive Order 10450.

The supervisor must advise the recipient of his/her responsibilities pertaining to the position to which assigned. The recipient should certify acknowledgement of these instructions and return the certification to this office.

This certification is not to be construed as a security clearance for access to classified information. If the need for a security clearance should arise, a written justification should be submitted to this office.

cc: Official Personnel Folder

DI 1917
Sept. 83

United States Department of the Interior

OFFICE OF SURFACE MINING
Reclamation and Enforcement
WASHINGTON, D.C. 20240

Memorandum

To: Alternate Security Officer

From:

Subject: Certification of Briefing for a Sensitive Position

I certify that I have been advised of and understand the responsibilities pertaining to the noncritical-sensitive/ critical-sensitive position to which I have been assigned; and that I will perform my duties in a responsible manner, adhering to standards.

_____ _____

Signature of Employee Date

United States Department of the Interior

OFFICE OF SURFACE MINING
Reclamation and Enforcement
WASHINGTON, D.C. 20240

Memorandum

To:

From: Alternate Security Officer

Subject: _____ - ADP Access Authorization

The investigative requirements for ADP positions established by 441 DM 6 have been accomplished. Based upon the information available, this individual's employment in the ADP position indicated below is consistent with the criteria established by FPM Chapter 732-9. This is not to be construed as a security clearance for access to classified information.

/___/ ADP-4 (Special-Sensitive)

/___/ ADP-3 (Critical-Sensitive)

/___/ ADP-2 (Nonsensitive-Critical)

/___/ ADP-1 (Non-Sensitive)

cc: Employee
Employee's OPF
Employee's Security File

DEPARTMENT OF THE INTERIOR
ADP ACCESS TERMINATION STATEMENT

NAME:_____ SSNo:_____

BUREAU/OFFICE_____ LEVEL OF ACCESS:_____

I am aware that by my signature below, I certify that the authorization for my access to ADP programs of the Department of the Interior is terminated. I am aware of my continuing responsibility for safeguarding the knowledge of ADP programs gained during my employment at the Department of the Interior.

_____
SIGNATURE OF EMPLOYEE

_____
SIGNATURE OF WITNESS

_____
DATE

Note: Complete this certification and return to the security office of record for ADP access authorization.

PRIVACY ACT NOTICE: In compliance with the Privacy Act of 1974, the following information is provided: Solicitation of the information requested on this form is authorized under Executive Order 10450. The purpose of this information is to confirm that the employee has been terminated from his/her access to Department of the Interior ADP programs. Routine use of this information may be by Federal, State and local agencies when relevant to security investigations and/or violations. Refusal to provide the requested information may result in appropriate administrative action and/or unauthorized exit clearance.