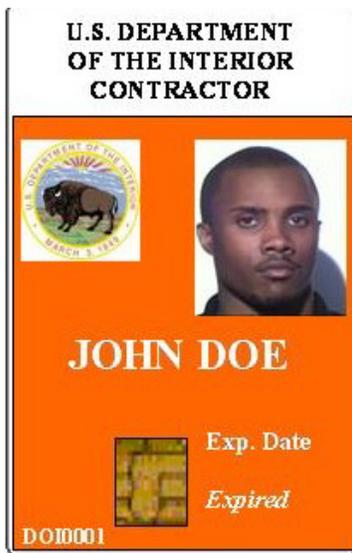
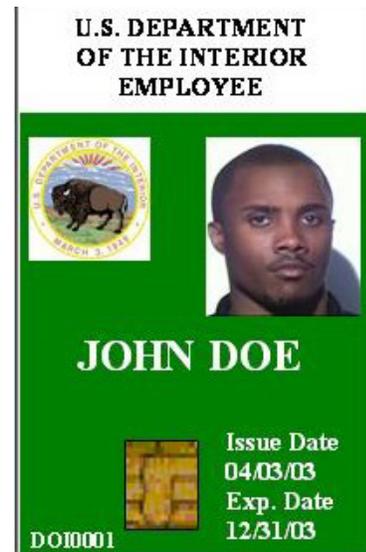




Computerized Identification Security System Procedures for Issuing and Using Smart Cards for Personal Identification



WO-850



DEPARTMENT OF THE INTERIOR
BUREAU OF LAND MANAGEMENT
WASHINGTON, D.C.

Computer ID Security System
Identification Card Issuance Procedures

Table of Contents

Introduction	3
Policy	3
Special Instructions	3
Hardware/Software Requirements	4
Responsibilities	4
Agency Head	4
Supervisors and Facility Managers	4
Departmental System Manager	5
State Office Computer ID System Administrator	5
Local System Monitor	5
Authorizing Official	6
Appointed Card Issuers	6
Smart Card Holders	6
Privacy	7
Information Gathering and Reporting	7
Request for information from the Enterprise Access Control System (Smart Card)	8
Card Issuance Infrastructure	8
Badge Station	9
Location	9
General Hours of Card Distribution	9
Type of System	9
Personnel Responsible for the System and Card Issuance	9
Enterprise Access Control System Log-in and Password/PIN	10
Requirements for Card Design	10
Card Issuance Procedures	11
Card Authorization	11
Permanent, Temporary, Term, Volunteer and Seasonal Employees	12
Contractors	12
Detailee	13
Retirees	14
Visitor Passes	14
Card Issuance for Collocating Facility	14
Lost or Stolen Cards	15
Process for Lost Cards	15
Repetitive Losses	15
Temporary Card for Lost Smart Cards	15
Left Card at Home	16
Extended Absences	16
Termination/Release of Employee	16
Washington, D.C. 20240	22
Illustrations	1-1
Illustrations	1-2
Illustrations	1-3
Illustrations	1-4
Illustrations	1-5

Computer ID Security System Identification Card Issuance Procedures

Introduction

The purpose of this directive is to establish standard procedures for identity and credentialing by the use of Smart Card Identification (ID) badges. This is the Department of the Interior (DOI) implementation of the Federal Identity Credential (FIC) required by the Office of Management and Budget (OMB). This will lead to a robust identity and authentication platform for non-repudiation of transactions for physical access to DOI facilities. These credentialing procedures will form the basis for future secure access to DOI computer networks and the use of electronic signatures.

These standards and procedures are established to ensure the integrity of Smart Card issuance in order to safeguard personnel from threats of danger, secure DOI facilities, allow for governmentwide interoperability, and adhere to established governmentwide, DOI requirements and policies.

Policy

The DOI has issued policy on credentialing activity standards and Smart Card acquisition requirements by the Office of the Chief Information Officer (OCIO) Directive 2004-008. The Smart Cards issued by Bureau Land Management (BLM) shall comply with the DOI policy. The DOI has declared that the DOI e-Authentication capability will employ a three-tier approach. Of the three approaches, Tier One defines the DOI physical access implementation. Tier one activity will include the establishment of secure (FIC), access controls, and authentication of DOI facilities, information systems, and networks supporting the requirements outlined in the Federal Information Security Management Act of 2002.

The Federal Identity Credentialing Committee has established minimum credential requirements for Smart Cards. The DOI Smart Card meets those requirements.

State and Field Offices will implement Smart Card usage for physical access to facilities and other secured areas. When released, State and Field Offices will issue digital certificates to employee Smart Cards for logical access to BLM information technology and equipment. In accordance with governmentwide goals and standards for credentialing and providing interoperability across government, BLM and its offices are required to follow DOI and other governmentwide policy and guidance as they are established. All BLM employees and contractors are to be issued ID Smart Cards by the end of calendar year 2004.

Special Instructions

Smart Card ID/badges are the property of the United States Government and will be issued to DOI employees, contractors, and certain collocating agency employees. The smart card shall be worn while in DOI owned or designated areas.

Computer ID Security System Identification Card Issuance Procedures

In order to maintain the integrity, respect, and acceptance of the Smart Card ID, the DOI will need to ensure that unauthorized personnel never has access to the card stock and equipment, that access privileges are updated expeditiously, that an employee never has more than one active ID/badge in his/her possession and is recovered from personnel who leave the agency.

Hardware/Software Requirements

All Smart Cards used for the Federal Identity Card, Issuance Stations, and Associated Parts must meet the specifications as indicated by GSC-IS (v2.1), along with the certification requirements of the Federal Bridge model, including all NIST recommended and approved standards and specifications such as FIPS 140-2.

Enterprise Access Control Systems (Smart Card Issuance Stations) and Associated Parts:

- 1) Must meet the GSC-IS (v2.1) requirements.
- 2) Must interface with the DOI's Enterprise Access Control System and meet requirements as indicated by the Certification and Accreditation process.
- 3) Must allow for interoperability across the DOI and other government agencies.
- 4) Must use the "contactless" chip for physical access and the contact chip for logical access.
- 5) Offices are to use GSC-IS (v2.1) Smart Cards or cards mandated by the BLM or OMB.

Responsibilities

Agency Head

The OMB requires Agency Heads to:

- 1) Oversee the control and use of Smart Card Issuance Stations and ID Cards within their Agency.
- 2) Take immediate action for persons violating this policy.
- 3) Establish internal procedures for card issuance, accessing the Enterprise Access Control System, and establish accountability of ID cards/badges.
- 4) Appoint an individual(s) with the appropriate security clearance to administer and maintain the integrity of the Smart Card E-Authentication Program.

Supervisors and Facility Managers

- 1) Ensure that any necessary employee union consultations/negotiations are conducted prior to instituting the Smart Card ID system or issuance of identity credentials, including issuance of any digital certificates.
- 2) Ensure that unauthorized personnel never has access to the card stock and equipment, that access privileges are updated expeditiously, that an employee never has more than one active ID card/badge in his/her possession and is recovered from personnel who leave the agency.
- 3) Ensure that employees authorized to issue the Smart Card IDs, computer system

Computer ID Security System
Identification Card Issuance Procedures

administrators, and any other person who may have access to the ID data base receive clearance for medium risk public trust as prescribed for personnel with routine access to privacy information. This requirement should be identified in the individual's position description.

- 4) Ensure that the individuals identified in number 3 above receive Privacy Act training specific to the ID system.
- 5) Document and make known to card issuer the criteria for issuing Smart Card IDs to employees of other agencies who may be collocated at BLM facilities.

Departmental System Manager

- 1) Responsible for completing confidential biannual audits verifying that procedures, policies, and proper documentation are enforced.
- 2) Ensure the quality and completeness (accuracy, consistency, and integrity) of data collections (data conversion, data cleanup, and conformance to established data standards) within each DOI Office or Bureau utilizing the DOI Computerized ID Security System.
- 3) Responsible for system and records maintenance and use as required by DOI and BLM guidance (BLM Manual Section 1270-1).
- 4) Must have a medium risk-public trust background investigation and security clearance to issue Smart Cards. The position description of the DOI System Manager shall include this requirement for a security clearance.
- 5) Requests and receives training on the application of the Privacy Act.

State Office Computer ID System Administrator

- 1) Responsible for completing confidential biannual audits verifying that procedures, policies, and proper documentation are enforced.
- 2) Responsible for providing statewide guidance for acquiring card issuance systems or client workstations, meeting or exceeding BLM and governmentwide standards and providing (printing) Smart Card solutions (where applicable).
- 3) Ensures the quality and completeness (accuracy, consistency and integrity) of data collections (data conversion, data cleanup, and conformance to established data standards) within each of his/her field district, collocated or other offices utilizing the DOI Computerized ID Security System within his/her State.
- 4) Coordinates with appropriate personnel to establish procedures and guidelines for monitoring physical security alarms disseminated from the Computerized ID Security System.
- 5) Must have a medium risk-public trust background investigation and security clearance to issue Smart Cards. The position description of the ID System Administrator shall include this requirement for a security clearance.
- 6) Requests and receives training on the application of the Privacy Act.

Local System Monitor

- 1) Responsible for monitoring all alarms from the Computerized ID Security System designated to him/her.
- 2) Follows BLM, DOI, and government policies and procedures for securing facilities and information.

Computer ID Security System
Identification Card Issuance Procedures

- 3) Maintains and provides detailed and accurate records of alarms to the State Office System Administrator or Designated Law Enforcement Official as deemed necessary by the local office security requirements.
- 4) Must have a medium risk-public trust background investigation and security clearance. The position description of the Local System Monitor shall include this requirement for a security clearance.
- 5) Requests and receives training on the application of the Privacy Act.

Authorizing Official (Approval Authority)

- 1) Knowledgeable of BLM standards for card issuance and Office of Personnel Management (OPM) and Federal Acquisition Regulations (FAR) for hiring and background investigations.
- 2) Responsible for verifying the cardholder identity, background checks, and other documentation as required by the BLM Human Resources Office, personnel Security Office, and OPM regulations.
- 3) Provides “permission” for applicant to receive a BLM SMART CARD provided that applicant meets or exceeds BLM requirements for employment (employee, contractor, temporary, term, etc.) by signing the approved request for ID form.
- 4) Appointed or delegated by the Agency Head.
- 5) Must have a medium risk-public trust background investigation and security clearances.

Appointed Card Issuers

- 1) Ensure that personnel requiring a Smart Card receive one and are properly briefed on this policy and any internal agency policies that outline user responsibility.
- 2) Ensure that proper breeder documentation is provided for individuals requesting Smart Cards.
- 3) Verify and validate cardholder identity prior to issuance.
- 4) Follow BLM and other governmentwide required procedures for card issuance.
- 5) Must have a medium risk-public trust background investigation and security clearance to issue Smart Cards. The position descriptions of card issuers shall include this requirement for a security clearance.
- 6) Request and receive training on the application of the Privacy Act.

Smart Card Holders

- 1) Shall safeguard their ID card. At no time will the card be loaned or borrowed.
- 2) Visibly wear the Smart Card at all times during work hours and while in DOI or BLM areas.
- 3) Promptly report the loss or theft of the Smart Card to the local card issuance office or their local office.
- 4) Immediately report to their supervisors or security the presence of unauthorized personnel in the work area.
- 5) Return the Smart Card to their Federal Identity Card Administrator or supervisor when placed in a non-work status or upon termination of employment.

Computer ID Security System
Identification Card Issuance Procedures

Privacy

Information gathered and entered into the DOI Computerized ID Security System (Smart Card) is covered by the DOI Privacy Act Notice (Interior/OS-01). The Agency Head and appointed individuals are responsible for protecting and maintaining the integrity of all data entered into the Computerized ID Security System.

Information Gathering and Reporting

All information gathered and reported in the Computerized ID Security System is covered by the Department of the Interior Privacy Act Notice (Interior/OS-01). Systems are required to capture data into the system for card issuance to new and existing applicants. Employees must complete an approved request for an ID form issued by the DOI, BLM, or BLM State Office (See Illustration 1-1). The approved forms and systems must contain the following minimum employee information in the required format:

- Official Name, Phone Number and Address of Office (Form only).
- Employee's First Name, Middle Initial, and Last Name--Employees are required to use name as indicated in the Federal Payroll System and all official records.
- Employee Social Security Number-xxx-xx-xxxx.
- Date of Birth--mm/dd/yyyy.
- Height--shall be written in feet and inches, example 5'3."
- Weight--Pounds.
- Eye Color--shall use the following options: Aqua, Black, Blue, Brown, Gray, Green, Hazel.
- Hair Color--Shall use the following options: Auburn, Bald, Black, Blond, Brown, Gray, Red, White, Other.
- Work Phone--xxx-xxx-xxxx.
- Type of Card Requested (Permanent, Temporary, Law Enforcement/Security, Contractor, Retiree, Volunteer).
- Expiration Date of the Card--mm/dd/yyyy.
- U.S. Citizenship Status.
If employee is not a U.S. citizen, they must provide the following: Country of Citizenship, Alien ID Card Number, Work Permit Number, and Expiration Date of Work Permit.
- Employee Signature (On the form only).
- Authorizing Official Signature and Printed Name.
- Bureau Office--Abbreviated, example BLM.
- Date--dd/mm/yyyy.
- Privacy Act Statement (Shall be displayed on the form; system shall display statement upon log-on).
- Contractor Information (See Card Issuance for Contractors below).

Computer ID Security System Identification Card Issuance Procedures

- Office Location: Shall include Bureau and official office name (as indicated in BLM Office Directory). Example, BLM-Arizona State Office or BLM-ID-Salmon Field Office. (Note: No spacing between “BLM-ID-Salmon.”) The BLM Washington Office shall distinguish offices by BLM-MIB and BLM-L Street.

Request for information from the Enterprise Access Control System (Smart Card)

The employee personal and access information in the system is covered by the DOI Privacy Act Notice. See the attached DOI Privacy Act Notice for additional information (Interior/OS-01) (See Illustration 1-3). In accordance with the notice, employee information, such as personal information and access information, is not to be disclosed to anyone outside of those listed in the notice. This information is not to be used for time and attendance reports.

Routine uses of the records maintained in the system, including the categories of users and the primary purpose of such uses of the system are:

- 1) To ensure the safety and security of DOI facilities and their occupants in which the system is installed.
- 2) To verify that all persons entering DOI facilities or other government facilities with Smart Card systems are authorized to enter them.
- 3) To track and control ID security cards issued to persons entering and exiting the facilities.
- 4) To provide physical access security to all employees. This information is not to be used for time and attendance reports.
- 5) Personnel must submit requests for information to the DOI Security Office.
(See Illustration 1-2)

Card Issuance Infrastructure

Issuance of the Federal Identity Card requires verification and validation of end user identity prior to issuance. Offices shall follow the BLM identity verification procedures as indicated by the Federal Identity and Credentialing Committee. Background investigations of criminal history, education certifications, credit history, work history, and other breeder documentation must meet BLM requirements before issuance. Card issuance is the process of distributing personalized cards to cardholders. Personalization may entail both logical and physical personalization of the card. Logical personalization involves transmittal and injection of the appropriate card applications, credentials, data, PIN and biometrics (if applicable) into the card application. Physical personalization of the card encompasses printing of the physical characteristics and security features on the surface of the card.

Computer ID Security System
Identification Card Issuance Procedures

Badge Station

No badging station (Smart Card Issuance Station), client workstation, or other component of the DOI Smart Card system is to be connected to the internet, either directly or indirectly or used for any other purpose and may not contain any software component that is not authorized by the Departmental System Manager. Smart Card issuance stations may only be installed at BLM Headquarters, State Offices, and Centers. Smart Cards will be printed by the State Office and issued to Field Offices using the following trust process:

- (1) Local office's Appointed Card Issuer will require that requesting employees complete the identity proofing process, request for ID form, and photo requirement as required in the card issuance procedures outlined in this document.
- (2) Local Appointed Card Issuer sends copies of request for ID forms, employee photos and log of requesting employees (displaying signature of Appointed Card Issuer) to State Office Appointed Card Issuer. The log shall include the requesting employee's name, office location, and Appointed Card Issuer's signature. Note: All digital employee photos (head shots) will be saved in jpeg format with a resolution of 640 x 480 or higher. File name formats should be saved as first name, last name, and last four digits of social security number or employee ID number. For example: John_Hancock1234.jpeg.
- (3) State Office sends printed Smart Cards, along with log of printed cards which displays signature of State Appointed Card Issuer through UPS, Federal Express, or trusted mailing process, requiring signature. The log shall include the printed cards, location where cards will be shipped, credentials added to card, and signature of State Appointed Card Issuer.
- (4) Local office signs for cards and requires that employees sign to receive their Smart Card.
- (5) Local office's Appointed Card Issuer will notify State Office of receipt of cards via email or faxed statement.

Each State Office shall establish a badging station location and office information. Field Offices shall establish a location and office information for client workstations. The following information shall be provided to the Property and Acquisition and Headquarters and Services group WO-850 and updated as needed:

- 1) **Location:** A secured location should be established for client workstation and/or monitoring system .
- 2) **General Hours of Card Distribution:** Offices will need to establish hours of operation. The BLM core hours of operation are from 9:30 a.m. to 3:30 p.m.
- 3) **Type of System:** Include software and hardware utilized.
- 4) **Personnel Responsible for the System and Card Issuance:**
 - a) State Office System Administrator.
 - b) Local System Monitor: Law Enforcement, Building Security or Federal Protective Services will need to monitor alarms from the system. Please indicate who monitors the alarms.

Computer ID Security System
Identification Card Issuance Procedures

- c) Authorizing Officials (Approving Authority): Offices will limit the number of Authorizing Officials to maintain integrity of information and access to facilities and information.

- d) Appointed Card Issuers: Offices should have a limited number of card issuers accessing the system. Recommend no more than three personnel.

Enterprise Access Control System Log-in and Password/PIN

Appointed Card Issuers, System Managers, and System Administrators will have individual log-ins and password/PINs for the system. The levels of access will be designated by the System Administrator. Individual log-ins will provide accountability and auditing records for the Agency Head, System Manager, and/or System Administrator.

- 1) System Auditing: The card issuance processes will be audited by the System Administrator and/or System Manager to ensure general compliance with BLM and DOI policy.
- 2) The process will include a biannual audit ensuring that the forms are accurately completed and signed by the authorized officials; expiration dates listed on the forms are concurrent with the information in the system, where required Smart Cards have been collected and access rights revoked, documentation of alarms, and logs are concurrent with system.

Requirements for Card Design

- 1) All BLM offices will use the badge formats designated by the DOI.
 - All cards will display the U.S. Department of the Interior name and logo, employee photo, the U.S. Government Statement of Property and Employee Accountability, 18 U.S.C 499 and 701, expiration date of card (with the exception of retiree cards), and the employee's official name as indicated in the Federal Payroll System.
- 2) Each employee will be issued the following card formats (See Illustration 1-4):
 - a) Permanent employees will be issued green badges. The expiration date of the Smart Card will be every five (5) years from the date of issue.
 - b) Temporary, Term, and Seasonal employees will be issued purple badges. Stickers denoting the expiration date of access are required for this badge type. The sticker and system expiration dates shall be updated yearly or by the terms of the temporary employee's need for access. The cards will be reprinted every five(5) years.
 - c) The BLM Law Enforcement/Security will be issued navy blue badges. The expiration date of the Smart Card will be every five (5) years from the time of issue.
 - d) Retired employees will be issued light blue badges upon request. These cards will not display an expiration date.
 - e) Contractors will be issued orange badges. Stickers denoting the expiration date of access are required for this badge type. The sticker and system expiration dates shall be updated yearly or by the terms of the contractor employee's need for access. The cards will be reprinted every five (5) years.
 - f) Volunteers will be issued a tan badge. Stickers denoting the expiration date of access are required for this badge type. The sticker and system expiration dates shall be

Computer ID Security System
Identification Card Issuance Procedures

updated yearly or by the terms of the contractor employee's need for access. The cards will be reprinted every five (5) years. Volunteers will receive badges on the basis of expected length of service and shall be provided at the discretion of the local office.

- g) Visitors will be issued a black badge or other card designated by the local office. Visitor cards can be used only at the issuing local office. See attached template.
- h) Administrator Badges for Logical Access Only: Administrators will be issued a pink access card for logical access use only in addition to their BLM Smart Card for temporary, contractor, and permanent employees. The Administrator card will display employee name, Administrator title, and Bureau. A picture shall not be displayed on the card. The Administrator Smart Card will be encoded for logical access only. The Administrators will not use these cards for physical access.

Card Issuance Procedures

Card Authorization

Authorizing Officials (Approving Authority) are the individuals who provide the Card Issuer permission to issue a card to a new (permanent, temporary, term, seasonal, and retiree), current (permanent, temporary, term, seasonal, and retiree), or contracting employee.

- 1) New Permanent, Term, Volunteer, Seasonal and Temporary Employees:
 - The authorized Approving Authority for New or Temporary Employees are the Personnel Officer/Specialist/Group that completes the Entry on Duty Process.
- 2) Contractor Employees:
 - a) The Authorized Signer for contractor employee badges must have access to contracting information to verify that a contract exists for the new contractor and the expiration of the contract. The Authorized Signer must also be able to verify that the required background check is listed in the contract and has been completed. The Authorized Signer may contact local law enforcement or personnel security to verify that the required background check as listed in the contract or required by position type has been conducted or is in process.
 - b) The Authorized Signer must ensure that contract information such as the contract number, expiration date of contract, company name, and contracting officer representative will be included on the approved Request for Identification Form.
 - c) The authorized Approving Authority will coordinate with Contracting Officer Representatives (CORs) to issue cards to contractor employees.
 - (1) Contracting Officers will need to provide a list of the current CORs to card issuance office and authorized Approving Authority. The CORs must be assigned to the contract to act on the contracted employees behalf for card issuance.
 - (2) The CORs are responsible for assisting contractors with the process for acquiring a Smart Card.
 - (3) The CORs are responsible for the return of contracted employees' Smart Cards to their local office at the expiration/termination of the contract.

Computer ID Security System
Identification Card Issuance Procedures

- (4) The CORs, along with contracted employee, are responsible for immediately notifying card issuance office of lost or stolen cards.
- (5) The CORs are responsible for acquiring extensions for access (must show proof of contract extension).
- (6) The CORs and Contracting Officers shall include a requirement for a background check in the contracts as required by Departmental, Bureau and governmentwide policy. The type of background check required is dependent upon the sensitivity of the position or tasks to be completed. The contracted employee may only require a non-sensitive background investigation, National Agency Check with Inquiry-NACI. The contract shall indicate the type of background investigation required.

Permanent, Temporary, Term, Volunteer and Seasonal Employees

- 1) Employee (applicant) must complete a DI-2005 or approved request for identification form.
- 2) Employee must have signature of Authorizing Official (Note: Signature indicates that employee has completed the Human Resources/Personnel Entry on Duty Process, is in the FPPS system, began or completed required background checks, and all required documentation has been submitted to Personnel and Personnel Security).
- 3) Employee must present proper ID (passport, State driver's license or identification card) and signed request for identification form to the Authorizing Official and Card Issuer.
- 4) New employee will need to be escorted by Supervisor or Personnel Officer to issuance office or the office should receive notification that new employee is reporting to office. If the employee is not escorted, they will need to show two forms of picture identification.
- 5) Temporary, Term, Volunteer and Seasonal Employees Smart Cards will have a sticker indicating the month and year of expiration. Upon extension of employment, the card will need to reflect the new date shown in the system. Dates of expiration for term, temporary and seasonal employees are not to exceed one year. Stickers and system should denote one year of access only. The date will need to be updated yearly. Dates of access cannot exceed the expiration date of the contract or appointment.
- 6) Termination or Resignation: Supervisor must notify Card Issuance Office immediately upon termination or resignation of employee. Employees completing final salary clearance process must surrender ID and receive clearance from Card Issuance Office.

Contractors

- 1) Contractor (applicant) must complete a DI-2005 or approved request for identification form.
- 2) Contractor must have signature of Authorizing Official.
 - a. The form shall indicate the contracting company, contract number, expiration date of the contract, and COR or Task Manager for the contract.
 - b. Authorizing Official shall confer with Contracting Officer to ensure that proper background investigation as indicated in the contract is complete.

Computer ID Security System
Identification Card Issuance Procedures

- c. Contractor must present proper ID (passport, State driver's license or State issued identification card) and signed forms to the Authorizing Official and Card Issuer. Contractor must present photo ID or provide two forms of identification.

- d. Contracting employee will need to be escorted by the COR or Supervisor to issuance office.
- e. Contractor badges will have a sticker indicating the month and year of expiration. Upon extension of contract, the card will need to reflect the new date shown in the system. Date of expiration for contracted employees is not to exceed one year. Stickers and system should denote one year of access only. The date will need to be updated yearly. Dates of access cannot exceed the expiration date of the contract.
- f. Contractor employees will not receive access to BLM facilities on Federal holidays and weekends. They will have BLM core hours of operation access, Monday through Friday, 6 a.m. to 6 p.m. The Contracting Officer or COR may request a change in access rights, which include extended access hours, weekend and Federal holiday access for the contracting employee by issuing a memorandum indicating the requested hours of access.
- g. Contract Extension: Contracting Officer will need to provide a notice indicating the new expiration date of the contract to the authorizing official, along with the completed request for ID form to extend the expiration date. When the employee's contract is extended, the COR or Contracting Officer will need to sign a new form with a new extended date.
- h. Termination of contract or contracting employee: Contracting Officer or COR must notify card issuance office immediately upon termination of contract or contracted employee. The ID must be returned to the COR or CO, who will then return the ID to the issuance office.

Detailee

Detailed employees may be issued a Smart Card outside of their home office provided that the required documentation is provided. If detailed employees are issued a new Smart Card, they will need to complete a DI-2005 or approved request for ID form and provide a memorandum from the sponsoring supervisor requesting access. The employee will need to include the expiration date of the visit on the form.

- 1) The request for ID form will be signed by the authorizing official at the visiting or home office. The authorizing official will verify employment status through the FPPS.
 - 2) The sponsoring supervisor will need to send electronic/fax to the Issuing Officer(s). The memorandum must include the name of employee, position/title, expiration date of new card, expiration date of detail or TDY, type of access required (24 hour or operating hours of 6 a.m. to 6 p.m.), type of employee, group number, home office code, sponsoring group manager and office/group number where employee will be detailed.
- a. Visiting office should issue a DI-105 to employee and employee's card issuance office. The DI-105 will include name of issuing office and serial number of old card

Computer ID Security System
Identification Card Issuance Procedures

- number. The DI-105 will also denote that the old identification card was exchanged for a new Smart Card. The DI-105 will indicate the value of the Smart Card for logical and physical access.
- b. The old card, copy of the request for ID form, and a copy of DI-105 will be returned to employee's home office (card issuance office).

Retirees

Upon retiring or renewal of a retiree's ID, the retired employee must provide the following:

- 1) Employee will need to provide a copy of SF-50 indicating retiree status to receive a retiree badge. Upon retiring, the employee is required to surrender current Smart Card or ID card to card issuance office.
- 2) If the employee is to receive retiree Smart Card prior to issuance of the SF-50, the Personnel Officer/Specialist (persons processing retiree status) will need to send a memorandum (electronically) to the card issuance office indicating that the employee has retired and requests a retiree ID. A copy of the SF-50 will need to be maintained with personnel. SF-50 must indicate retiree status.
- 3) The applicant must obtain signature of Authorized Signer.
- 4) If the retiring employee did not receive a retiree ID when they returned their employee ID, then they will have to submit a completed and signed DI-2005 from personnel.

Visitor Passes (Office Specific)

Complete approved visitor request for access form.

- 1) Visitor cards do not have a photo. They are standard printed cards with "Visitor" printed on them only. These cards can be reissued to other visitors.
- 2) Visitor cards may only be used at the issuing office. They are not valid for other facilities.
- 3) Submit copy of ID (unless already on file).
- 4) Signature of person (s)/sponsor being visited must be listed on the form or in the office log.
- 5) All visits using the Smart Card systems must be official business to receive a visitor card; otherwise, all other visitors should be escorted by person(s) being visited.
- 6) Visitor form must list areas and hours of access.
- 7) Visitor passes are not to exceed five business days. They may be renewed every five business days.

Card Issuance for Collocating Facility:

Offices are to establish a service agreement to issue Smart Card ID cards for the U.S. Department of Agriculture Forest Service employees or other agencies that collocate with BLM offices. The agreement will need to include the cost of the cards. The agreement will also include the responsibilities of the recipients of the cards, the receiving agency and the issuing agency.

- 1) Purpose of the agreement is to establish official guidance for card issuance at the collocated facility. Guidance will also help alleviate redundancy in Smart Card printing and provide cost savings to all agencies involved. Employees of other

Computer ID Security System
Identification Card Issuance Procedures

agencies should be able to use their Smart Cards at their agency's facilities that have Smart Card systems.

- 2) These agreements will also further the goals of governmentwide interoperability and identification and credentialing of employees.

Lost or Stolen Cards

Process for Lost Cards

- 1) Employee must report any lost card immediately to the card issuance office. The card issuance office will denote loss in the system by changing the credential issue level. All newly issued cards must be accounted for in the system. A notation shall be placed in the system indicating the date the card was reported lost and the initials of the appointed card issuer. A notation shall also be placed in the system indicating the date a new card was issued and the initials of the appointed card issuer. Employees may be held accountable for lost or stolen property as result of not reporting lost or stolen Smart Cards. Such findings will be reported to the Board of Survey for determination.
- 2) Employee must sign in lost card log to report lost card immediately. A 10-day waiting period begins with date logged as stolen or lost and submittal of "Replacement ID form." The purpose of the 10-day waiting period is to allow for the return of card. In many cases, lost cards are found or mailed to the DOI and can be reissued to the employee.
- 3) Employee must complete the approved Replacement/Lost Card Form.
- 4) Employee must obtain signature of Supervisor (signifying current employee and acknowledgement of lost card), designated Security Officer or Law Enforcement and Smart Card Security Representative.
- 5) Employee must show photo ID (State issued driver's license or ID card and/or passport).

Repetitive Losses

- 1) First reported loss - Follow Standard procedure for lost/stolen card.
- 2) Second reported loss - Follow Standard procedure for lost/stolen card. Group or Program will be required to pay for replacement of card.
- 3) Three or more lost cards - Follow Standard procedure for lost/stolen card and complete a Report of Survey for negligence. The Board of Survey may require that the employee pay for a lost card.

Temporary Card for Lost Smart Cards

- 1) Temporary cards do not have a picture on the cover. They are used for local building access only. The temporary card is for use in the building where issued only. This card cannot be used at other offices across the BLM or other government agencies.
- 2) Employee will be issued a temporary card for building access during the 10-day waiting period.

Computer ID Security System
Identification Card Issuance Procedures

- 3) The approved card issuer will restrict employees from using the temporary card for access after 10 days.
- 4) Employees are held accountable for temporary cards as well.
- 5) Process for Stolen Cards.
 - a) Employee is required to submit a copy of the police report for the stolen Smart Cards. If the card is stolen, employee will be issued a new card immediately.
 - b) If proof that card was stolen is not provided, the employee will be required to follow procedures for lost cards.

Left Card at Home (Temporary Card)

The cardholder must complete request for temporary ID for physical access or return to residence to pick up.

- (1) Obtain the following signatures: Employee Signature, Group Manager, Designated Security Officer and Card Issuance Office. Employees are required to have on display an official government ID at all times while on government property. Offices may limit access of employee to front door and office (desk) space only.

Extended Absences

If an employee will be absent 30 days or more due to an extended illness, military service, seasonal employment, detail, etc., but will return at a later time, they must notify their local card issuance office, so that access rights may be temporarily suspended.

Termination/Release of Employee

Final Salary Clearance

- 1) All employees must clear with the Final Salary Clearance form established for their office.
- 2) All Permanent/Temporary/Contracted employees must clear with the Smart Card office to relinquish access to facility. Card issuers are required to change status of card to inactive. A notation should be placed in the system indicating if the card was returned and that the employee was released.
- 3) Permanent Employee must surrender current ID. Card issuers are required to change status of card to inactive. A notation should be placed in the system indicating if the card was returned and that the employee was released.
- 4) Retiring employee must surrender current permanent employee ID (green) and complete the request for ID signed by the authorizing official indicating retired employee status to obtain retiree card (light blue card). The authorizing official must view a copy of the SF-50 or receive notice from Personnel Office that the employee has retired.
- 5) Temporary and Contractors: The cardholder must surrender the ID card. (Please notify office if employee will return at a later time. The Smart Card will be deactivated and kept on file.) Card issuers are required to change status of card to inactive. A notation should be placed in the system indicating if the card was returned and that the employee was released.

Computer ID Security System
Identification Card Issuance Procedures

- 6) If the employee transfers to a new office, the employee will need to provide a copy of the confirmation of their new appointment within BLM or DOI to their current office. The employee's Smart Card forms/documents will need to be mailed directly to the Smart Card issuance office to which the employee is reporting. The current office will also deactivate access rights to the facility and transfer the cardholder record (within the system) to the new office. The new office will need to update the employee information and grant access to its facilities and/or systems. This process will permit the current office to release the ID from the Final Salary Clearance Process and transfer the ID to the new office.

Computer ID Security System
ID Card Issuance Procedures

U.S. Department of the Interior
Request for Identification Card

When completed, submit to the Security Services Branch located in room 1229, Main Interior Building.
Telephone – 202.208.5111/5112 Fax – 202.208.7610 E-mail – Security_Services@ios.doi.gov

Please issue an identification card to the following individual: (print clearly or type).

Name: _____
Last First Middle

SSN: _____ DOB: _____ Height: _____ Weight: _____

Eye Color: _____ Hair Color: _____ Work Phone: _____

Type of Card Requested: (Check One)

Permanent Employee _____ Temporary Employee _____ (Volunteer, Student) Expiration Date: _____

LENF _____ Security _____ Emergency Mgt. _____

OGA _____ Retiree ID _____ Car-pool _____

This badge is the property of the Department of the Interior and must be surrendered to the Security Services Branch upon demand or termination of employment. It MUST be visibly displayed at all times while on Department of the Interior property. Report lost or stolen badge immediately to the Security Services Branch. **A replacement fee may be assessed.** The counterfeiting, alteration, or misuse is a violation of 18 U.S.C. 499 and 701.

Privacy Act Statement

Section 301 of Title 5 to the U.S. Code authorizes collection of this information. The Primary use of this information is by Employee and Public Services and the Security Services Branch to approve and issue your official Department of the Interior identification card. Maintenance and disclosure of the information collected by means of this form is governed by the Department of the Interior system of records notice for Computerized ID Security System – Interior/OS-01.

Where we have asked you for your Social Security Number, collection of this information is authorized by Executive Order 9397. Furnishing the information on this form, including your Social Security Number, is voluntary, but failure to do so may result in disapproval of this request. If the Department of the Interior uses the information furnished on the form for purposes other than referred to above, it may provide you with an additional statement reflecting those purposes.

By signing this document, the employee accepts responsibility for a Department of the Interior ID Badge. The ID Badge is U.S. Government Property and should be treated as such.

Employee's Signature

DOI Authorizing Official's Signature

Date

Bureau/Office

Authorizing Official's Name (Print)

Phone Number

Computer ID Security System
ID Card Issuance Procedures

U.S. Department of the Interior
Contractor Request for Access

Modernization Contractor: _____ Non-Modernization Contractor: _____

When completed, submit to the Security Services Branch located in room 1229, Main Interior Building.

Telephone: 202-208-5111/5112

Fax: 202-208-7610

E-mail:

Security_Services@nbc.gov

Please print clearly or type. This form will be returned if there are any unanswered questions. Please follow format below to ensure timely processing.

Name: _____
Last First
Middle

SSN: _____ - _____ - _____ DOB: ____/____/____ Height: _____ Weight: _____

Eye Color: _____ Hair Color: _____ U.S. Citizen: _____ Yes _____ No*
*If no fill out bold questions

Country of Citizenship: _____ **Alien ID Card Number:** _____

Work Permit Number: _____ **Expiration Date:** _____

Company Name: _____ Telephone: _____

Company Point of Contact: _____

Company Address _____

Expiration Date: _____ (NTE One Year) DOI Contact (CO/COTR): _____

Contract Number: _____ Contract Expiration Date: _____

This badge is the property of the Department of the Interior and must be surrendered to the Security Services Branch upon demand or termination of employment. It MUST be visibly displayed at all times while on Department of the Interior property. Report lost or stolen badge immediately to the Security Services Branch. **A replacement fee may be assessed.** The counterfeiting, alteration, or misuse is a violation of 18 U.S.C. 499 and 701.

Privacy Act Statement

Section 301 of Title 5 to the U.S. Code authorizes collection of this information. The Primary use of this information is by Employee and Public Services and the Security Services Branch to approve and issue your official Department of the Interior identification card. Maintenance and disclosure of the information collected by means of this form is governed by the Department of the Interior system of records notice for Computerized ID Security System – Interior/OS-01.

Where we have asked you for your Social Security Number, collection of this information is authorized by Executive Order 9397. Furnishing the information on this form, including your Social Security Number, is voluntary, but failure to do so may result in disapproval of this request. If the Department of the Interior uses the information furnished on the form for purposes other than referred to above, it may provide you with an additional statement reflecting those purposes.

By signing this document, the contractor accepts responsibility for a Department of the Interior ID Badge. The ID Badge is U.S. Government Property and should be treated as such.

Computer ID Security System
ID Card Issuance Procedures

Contractor's Signature

DOI Authorizing Official's Signature

Date

Bureau/Office

Authorizing Official's Name (Print)

Phone Number

Computer ID Security System
ID Card Issuance Procedures
U.S. Department of the Interior
Request for Replacement of Lost or Damaged ID Card

When completed, submit to the Security Services Branch located in room 1229, Main Interior Building.
Telephone – 202.208.5111/5112 Fax – 202.208.7610 E-mail – Security_Services@ios.doi.gov

Please issue an identification card to the following individual: (print clearly or type).

Name: _____
Last
First
Middle

SSN: _____ Reason for Request: Lost / Damaged

Type of Replacement Card Requested: (Check One)

Permanent Employee _____ Temporary Employee _____ (Volunteer, Student) Expiration Date: _____

LENF _____ Security _____ Emergency Mgt. _____

OGA _____ Retiree ID _____ Car-pool _____

Contractor _____

This badge is the property of the Department of the Interior and must be surrendered to the Security Services Branch upon demand or termination of employment. It MUST be visibly displayed at all times while on Department of the Interior property. Report lost or stolen badge immediately to the Security Services Branch. **A replacement fee may be assessed.** The counterfeiting, alteration, or misuse is a violation of 18 U.S.C. 499 and 701.

Privacy Act Statement

Section 301 of Title 5 to the U.S. Code authorizes collection of this information. The Primary use of this information is by Employee and Public Services and the Security Services Branch to approve and issue your official Department of the Interior identification card. Maintenance and disclosure of the information collected by means of this form is governed by the Department of the Interior system of records notice for Computerized ID Security System – Interior/OS-01.

Where we have asked you for your Social Security Number, collection of this information is authorized by Executive Order 9397. Furnishing the information on this form, including your Social Security Number, is voluntary, but failure to do so may result in disapproval of this request. If the Department of the Interior uses the information furnished on the form for purposes other than referred to above, it may provide you with an additional statement reflecting those purposes.

By signing this document, the employee’s supervisor acknowledges that the replacement cost of the smart card is the responsibility of the employee’s bureau. The ID Badge is U.S. Government Property and should be treated as such.

Employee Signature

Employee’s Supervisor’s Signature

Date

Bureau/Office

Supervisor’s Name (Print)

Phone Number

Security Chief Approval

Computer ID Security System
ID Card Issuance Procedures



U.S. Department of the Interior
National Business Center Security Services

Washington, D.C. 20240

Request for Release of Entrance Logs*

Requestor: (print/sign) _____

Badge Number: _____

Agency: _____

Date of Request: _____

Purpose of Request: _____

DOI Security Incident Report Number: _____

FPS Report Number: _____

Date(s) and Time(s): _____

Employee / Visitor / All

Format: Paper / Diskette

Number of Copies: _____

Recipient(s) of Copies / Purpose:

Computer ID Security System
ID Card Issuance Procedures

*All information is protected by the Privacy Act of 1974

Computer ID Security System
ID Card Issuance Procedures

Privacy Act of 1974

NARRATIVE STATEMENT FOR AN AMENDED SYSTEM OF RECORDS FOR THE
DEPARTMENT OF THE INTERIOR COMPUTERIZED ID SECURITY SYSTEM

Computerized ID Security System, Interior, OS-01

This revised system of records contains information on individuals with smart card IDs who have had access to Department of the Interior (DOI) facilities with smart card access control systems installed. The current access control system is only installed in the Main Interior complex in Washington, DC. It is being replaced by a smart card system and expanded to other DOI facilities. The new Computerized ID Security System will be able to link all DOI facilities nationwide. The new system will have the capacity for 500,000 user records, but will be primarily for the 70,000 DOI employees and contractors and visitors from within and outside the Government. The information collected will be used to identify individuals and grant/deny access to DOI facilities. This system of records is maintained under the authority of 5 U.S.C. 301 and the Presidential Memorandum on Upgrading Security at Federal Facilities, June 28, 1995. The system is maintained by NBC Security Services, and includes all the information collected from all DOI locations that use the smart card system.

This system of records will be used to monitor the entry/exit of individuals at DOI facilities with smart card access control systems installed. The DOI will share information in this system of records with other agencies that have adopted a smart card access control system for their facilities. When an individual from another agency requests access to a DOI facility with the smart card access control system, or a DOI employee requests access to another agency's facilities, the individual's information will be exchanged between the access control systems.

Security access to data covered by this system of records is available at all locations within DOI locations (both Federal buildings and Federally-leased space) where staffed guard stations have been established in facilities that have installed the smart card access control system, as well as the physical security office of those locations. Access granted to individuals at guard stations is password-protected and users' access to the data will be limited by the access rights that are assigned to their password. The screen displaying information is protected from view by unauthorized users when located at guard stations or in offices with employees who do not have a need to know the information.

Access granted to individuals is password-protected; each person granted access to the access control system must be trained and individually authorized to use the access control system. All users of the access control system are required to follow established internal security protocols. Performance of contract employees is monitored. The users' access to the data will be limited by the access rights that are assigned to their password. The physical security staff will be able to add/delete records, search the data base for particular items, print reports, and grant/deny access to specific entrance/exit locations. The guards that staff the guard post will be limited to verifying the access rights of a person seeking entry into the facility.

Computer ID Security System ID Card Issuance Procedures

Two new routine uses have been added to the system of records to allow DOI to disclose information to both: (1) other agencies that have similar smart card access control systems, when a DOI smart card holder desires access to that agency's facility; and (2) to an official of another Federal agency to provide information needed in the performance of official duties related to reconciling or reconstructing data files, in support of the functions for which the records were collected or maintained. Additionally, the text and/or scope of the five original routine uses have been modified to varying degrees.

This proposal does not require any new or revised rules to be published in the Federal Register; it only changes the scope of the records that are collected and maintained.

Computer ID Security System
ID Card Issuance Procedures

4310-94-M

DEPARTMENT OF THE INTERIOR

Office of the Secretary

Privacy Act of 1974, As Amended; Amendment of an Existing System of Records

AGENCY: U.S. Department of the Interior

ACTION: Proposed amendment of an existing system of records

SUMMARY: The Department of the Interior (DOI) is issuing public notice of its intent to amend a Privacy Act (PA) system of records in its inventory of records systems subject to the Privacy Act of 1974 (5 U.S.C. 552a). Interior/OS-01, "Computerized ID Security System" is being amended because DOI, Office of the Secretary, National Business Center, is replacing its current computerized access control system with a new "Smart Card" access control system. The current access control system is used to maintain access control to the Main Interior complex in Washington, DC. The new access control system will be used to maintain access control to all DOI facilities that have installed smart card access control systems. In addition to the information collected under the current access control system, the new access control system will record the entry/exit locations, access status, and personal identification numbers (PIN) of the smart card holder. Two new routine uses have been added to the system of records to allow DOI to disclose information to both: (1) other agencies that have similar smart card access control systems, when a DOI smart card holder desires access to that agency's facility; and (2) to an official of another Federal agency to provide information needed by that agency in the

Computer ID Security System
ID Card Issuance Procedures

performance of official duties related to reconciling or reconstructing data files, in support of the functions for which the records were collected or maintained. Additionally, the text and/or scope of the five original routine uses have been modified to varying degrees. The data will be stored on a server located in the Main Interior building in Washington, DC, with a backup server located in the DOI National Business Center facility in Denver, CO. Data exchanged between the servers and between the servers and the client PCs will be encrypted.

EFFECTIVE DATE: 5 U.S.C. 552a (e) (11) requires that the public be provided a 30-day period in which to comment on the agency's intended use of the information in the system of records. The Office of Management and Budget, in its Circular A-130, requires an additional 10-day period (for a total of 40 days) in which to make these comments. Any persons interested in commenting on this proposed amendment may do so by submitting comments in writing to the Office of the Secretary Privacy Act Officer, Sue Ellen Sloca, U.S. Department of the Interior, Mail Stop (MS)-1414- Main Interior Building (MIB), 1849 C Street, NW, Washington, DC 20240, or by e-mail to Sue_Ellen_Sloca@nbc.gov. Comments received within 40 days of publication in the Federal Register will be considered. The system will be effective as proposed at the end of the comment period unless comments are received which would require a contrary determination. The Department will publish a revised notice if changes are made based upon a review of comments received.

FOR FURTHER INFORMATION CONTACT: David VanderWeele, Security Specialist, NBC Security Services, MS-1229, 1849 C St., NW, Washington, DC 20240 (David_A_Vanderweele@nbc.gov).

Computer ID Security System
ID Card Issuance Procedures

A copy of the system notice for OS-01, Computerized ID Security System, follows.

Dated:

Sue Ellen Sloca

Office of the Secretary Privacy Act Officer

Department of the Interior

Computer ID Security System
ID Card Issuance Procedures

Interior Department – Privacy Act Notice

INTERIOR/OS-01

System name: Computerized ID Security System – Interior, OS-01

System location: (1) Data covered by this system are maintained in the following locations: U.S. Department of the Interior, Office of the Secretary, National Business Center, Computer Center, 1849 C Street, NW, Washington, DC 20240; U.S. Department of the Interior, Office of the Secretary, National Business Center, 7301 W Mansfield Ave, MS D-2130, Denver, CO 80235-2300. (2) Limited access to data covered by this system is available at Department of the Interior (DOI) locations, both Federal buildings and Federally-leased space, where staffed guard stations have been established in facilities that have installed the smartcard ID system, as well as the physical security office(s) of those locations.

Categories of individuals covered by the system: All individuals who have had access to DOI facilities that have the smartcard access control system installed. These include, but are not limited to, the following groups: current agency employees, former agency employees, agency contractors, persons authorized to perform or use services provided in DOI facilities (e.g., Department of the Interior Federal Credit Union, Interior Department Recreation Association Fitness Center, etc.), other Government employees from agencies with smartcard systems, volunteers, and visitors.

Categories of records in the system: Records maintained on current agency employees, former agency employees, and agency contractors include the following data fields: Name, Social Security number, date of birth, signature, image (photograph), hair color, eye color, height, weight, organization/office of assignment, telephone number of emergency contact (optional/voluntary data field), date of entry, time of entry, location of entry, time of exit, location of exit, security access category, access status, personal identification number (PIN), number of ID security cards issued, ID security card issue date, ID security card expiration date, and ID security card serial number. Records maintained on all other individuals covered by the system include the following data fields: Name, Social Security number (or one of the following: Driver's License number, "Green Card" number, Visa number, or other ID number), U.S. Citizenship (yes or no/logical data field), date of entry, time of entry, location of entry, time of exit, location of exit, purpose for entry, agency point of contact, company name, security access category, access status, personal identification number (PIN), number of ID security cards issued, ID security card issue date, ID security card expiration date, and ID security card serial number.

Authority for maintenance of the system: 5 U.S.C. 301; Presidential Memorandum on Upgrading Security at Federal Facilities, June 28, 1995.

Routine uses of records maintained in the system including categories of users and the purposes of such uses: The primary purposes of the system are:

Computer ID Security System
ID Card Issuance Procedures

- (1) To ensure the safety and security of DOI facilities and their occupants in which the system is installed.
- (2) To verify that all persons entering DOI facilities or other Government facilities with smartcard systems are authorized to enter them.
- (3) To track and control ID security cards issued to persons entering and exiting the facilities.

Disclosures outside the DOI may be made:

- (1) To an expert, consultant, or contractor (including employees of the contractor) of DOI that performs, on DOI's behalf, services requiring access to these records.
- (2) To the Federal Protective Service and appropriate Federal, State, local or foreign agencies responsible for investigating emergency response situations or investigating or prosecuting the violation of or for enforcing or implementing a statute, rule, regulation, order or license, when DOI becomes aware of a violation or potential violation of a statute, rule, regulation, order or license.
- (3) To another agency with a similar smart card system when a person with a smart card desires access to that agency's facilities.
- (4)(a) To any of the following entities or individuals, when the circumstances set forth in (b) are met:
 - (i) The Department of Justice (DOJ);
 - (ii) a court, adjudicative or other administrative body;
 - (iii) a party in litigation before a court or adjudicative or administrative body; or
 - (iv) any DOI employee acting in his or her individual capacity if DOI or DOJ has agreed to represent that employee or pay for private representation of the employee;
- (b) When
 - (i) One of the following is a party to the proceeding or has an interest in the proceeding:
 - (A) DOI or any component of DOI;
 - (B) any DOI employee acting in his or her official capacity;
 - (C) any DOI employee acting in his or her individual capacity if DOI or DOJ has agreed to represent that employee or pay for private representation of the employee;
 - (D) the United States, when DOJ determines that DOI is likely to be affected by the proceeding; and
 - (ii) DOI deems the disclosure to be:
 - (A) relevant and necessary to the proceeding; and
 - (B) compatible with the purposes for which the records were compiled.
- (5) To a congressional office in response to an inquiry an individual covered by the system has made to the congressional office about him or herself.
- (6) To an official of another Federal agency to provide information needed in the performance of official duties related to reconciling or reconstructing data files, in support of the functions for which the records were collected and maintained.
- (7) To representatives of the General Services Administration or the National Archives and Records Administration to conduct records management inspections under the authority of 44 U.S.C. 2903 and 2904.

Computer ID Security System ID Card Issuance Procedures

Note: Disclosures within DOI of data pertaining to date and time of entry and exit of an agency employee working in the District of Columbia may not be made to supervisors, managers or any other persons (other than the individual to whom the information applies) to verify employee time and attendance record for personnel actions because 5 U.S.C. 6106 prohibits Federal Executive agencies (other than the Bureau of Engraving and Printing) from using a recording clock within the District of Columbia, unless used as a part of a flexible schedule program under 5 U.S.C. 6120 et seq.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:

Storage: Records are stored in electronic media and in paper files.

Retrievability: Records are retrievable by name, Social Security number, other ID number, image (photograph), organization/office of assignment, agency point of contact, company name, security access, category, date of entry, time of entry, location of entry, time of exit, location of exit, ID security card issue date, ID security card expiration date, and ID security card serial number.

Access Safeguards: The computer servers in which records are stored are located in computer facilities that are secured by alarm systems and off-master key access. The computer servers themselves are password-protected. Access granted to individuals at guard stations is password-protected; each person granted access to the system at guard stations must be individually authorized to use the system. A Privacy Act Warning Notice appears on the monitor screen when records containing information on individuals are first displayed. Data exchanged between the servers and the client PCs at the guard stations and badging office are encrypted. Backup tapes are stored in a locked and controlled room in a secure, off-site location.

Retention and disposal: Records relating to persons covered by this system are retained in accordance with General Records Schedule 18, Item No. 17. Unless retained for specific, ongoing security investigations:

(1) Records relating to individuals other than employees are destroyed two years after ID security card expiration date.

(2) Records relating to date and time of entry and exit of employees are destroyed two years after date of entry and exit.

(3) All other records relating to employees are destroyed two years after ID security card expiration date.

System manager(s) and address: Security Manager, Physical Security Office, Division of Employee and Public Services, National Business Center, MS-1224, 1849 C Street, NW, Washington, DC 20240.

Notification procedures: An individual requesting notification of the existence of records on himself or herself should address his/her request to the Security Manager. The request must be in writing and signed by the requester. (See 43 CFR 2.60.)

Computer ID Security System
ID Card Issuance Procedures

Records access procedures: An individual requesting access to records maintained on him or herself should address his/her request to the Security Manager. The request must be in writing and signed by the requester. (See 43 CFR 2.63.)

Contesting record procedures: An individual requesting amendment of a record maintained on himself or herself should address his/her request to the Security Manager. The request must be in writing and signed by the requester. (See 43 CFR 2.71.)

Record source categories: Individuals covered by the system, supervisors, and designated approving officials.

Exemptions claimed for the system: None.

Computer ID Security System
ID Card Issuance Procedures

Department of the Interior ID Badge Formats

