Minerals Management Service
Interim Policy Document

Effective Date: November 30, 2005 **IPD No. 06-03**
Series: Administrative
Title: Personal Identity Verification Credential

Originating Office: Chief of Staff for Administration and Budget

1. Purpose. This Interim Policy Document (IPD) establishes policy and provides procedures for the issuance of a standard Minerals Management Service (MMS) identification card through the use of Homeland Security Presidential Directive – 12 (HSPD-12) compliant Personal Identity Verification (PIV) credentials, hereafter referred to as the PIV credential or card.

2. Objectives.

A. This is the MMS implementation of the Federal Identity Credential required by the Office of Management and Budget (OMB) which will result in a robust identity and authentication platform for nonrepudiation of transactions for physical access to MMS facilities. These credentialing procedures will form the basis for future secure access to bureau-controlled information systems and the use of electronic signatures. The PIV credential will be used as the standard MMS identification and will replace the DI-238 and DI-238A identification cards no later than October 27, 2007.

B. These standards and procedures are established to ensure the integrity of PIV credential issuance as a means to safeguard personnel from threats of danger, secure MMS facilities, assimilate government-wide interoperability, and to adhere to established government-wide and Department of the Interior (DOI) requirements and policies. This IPD supplements the MMS Manual, Part 310.1, Identification Cards, and will replace the chapter once the bureau fully migrates to the PIV credential.

3. Authority.

A. Homeland Security Presidential Directive 12 (HSPD-12).

B. Federal Information Processing Standards Publication 201 (FIPS PUB 201).

4. References.

A. Privacy Act of 1974.

B. OMB Memorandum, Implementation of Homeland Security Presidential Directive - 12 - Policy for a Common Identification Standard for Federal Employees and Contractors, August 5, 2005.

C. OMB Memorandum, Streamlining Authentication and Identity Management within the Federal Government, July 3, 2003.

D. OMB Directive 115-0136, Employment Eligibility Verification.

E. National Institute of Standards Special Publication 800-79, Guidelines for the Certification and Accreditation of PIV Card Issuing Organizations.

F. DOI, OCIO Directive 2004-008.

G. DOI, Assistant Director, Office of Law Enforcement and Security, Memorandum, Definition of Card Issuance and Facility Guidance Regarding HSPD-12, July 14, 2005.

H. DOI, Assistant Director, Office of Law Enforcement and Security, Memorandum, Guidance Regarding Installation of Smart Card Readers at DOI Facilities, May 25, 2005.

I. DOI, Assistant Director, Office of Law Enforcement and Security, Memorandum, Interim Guidance Background Investigations of Contract Employees, January 31, 2005.

J. MMS Manual, Part 310, General, Security, Chapter 1, Identification Cards.

5. Background. In response to HSPD-12, the National Institute of Standards and Technology (NIST) published *Federal Information Processing Standards Publication 201* (FIPS 201) on February 25, 2005. FIPS 201 and its associated Special Publications provide a detailed specification for Federal agencies and departments deploying the PIV credential for their employees and contractors. Once implemented, a secure and interoperable PIV credential will provide the attributes of security, authentication, identity verification, trust, and privacy to a commonly accepted identification card for Federal employees and contractors. Physical access control rights granted to the PIV credential will remain a local agency decision. The PIV credential is a core component to setting the "trust model" across the Federal enterprise.

6. Definitions.

A. Federal employee, as defined in title 5 U.S.C §2105 "Employee." For the purpose of this title, "employee" means an officer or an individual who is:

(1) Appointed in the civil service by one of the following acting in an official capacity:

(a) The President.

(b) A Member or Members of Congress, or the Congress.

(c) A member of a uniformed service.

(d) An individual who is an employee under this section.

(e) The head of a Government controlled corporation.

(f) An adjutant general designated by the Secretary concerned under section 709(c) of title 32.

(2) Engaged in the performance of a Federal function under authority of law or an Executive act.

(3) Subject to the supervision of an individual named by paragraph (1) of this subsection while engaged in the performance of the duties of his position.

B. Contractor is an individual under contract to MMS who is affiliated with MMS in excess of 180 calendar days and who requires unsupervised access to bureau controlled information systems and facilities.

C. Other authorized individual includes interns, guest researchers, tribal users, volunteers, intermittent, temporary or seasonal employees who are affiliated with MMS in excess of 180 calendar days and who require unsupervised access to bureau-controlled information systems and facilities.

D. Federally Controlled Information System.

(1) Information technology system (or information system), as defined by the Federal Information Security Management Act of 2002, (44 U.S.C. §3502(8)).

(2) Information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency as defined in 44 U.S.C. §3544(a)(1)(A).

E. Federally Controlled Facility.

(1) Federally-owned or leased space, whether for single or multi-tenant occupancy, including grounds and approaches, all or any portion of which is under the jurisdiction, custody or control of a department or agency covered by the provisions of HSPD-12.

(2) Federally controlled commercial space shared with non-government tenants. For example, if a department or agency leased the 10th floor of a commercial building, the provisions of this Directive apply to the 10th floor only.

F. Background Investigation is an examination of an individual's personal history over a predefined period of time to determine his suitability for a position with the Federal government. Background investigations are conducted by the Office of Personnel Management (OPM) and examine an individual's reputation, loyalty, trustworthiness, qualifications, and other pertinent factors. The type and scope of the investigation conducted is determined by the duties and responsibilities of the position.

G. National Agency Check (NAC) is a preliminary investigation, limited and specific in scope, conducted by OPM as part of a full background investigation. The NAC consists of a search of OPM and Department of Defense background investigation files and an FBI National Criminal History Fingerprint check.

H. Supervised physical and logical access for purposes of this IPD means that an individual must be escorted at all times while in an MMS-controlled facility and directly monitored while viewing any bureau-controlled information system.

7. Policy. HSPD-12 directs the promulgation of a new Federal standard for secure and reliable identification issued by Federal agencies for their employees and contractors. The DOI has issued policy on credentialing activity standards and PIV credential acquisition requirements by the Office of the Chief Information Officer (OCIO) Directive 2004-008. The credentials issued by MMS will be compliant with HSPD-12 and the OCIO Directive. Completion of the PIV credential issuing process will be completed across the bureau no later than October 27, 2007.

8. Responsibilities.

A. Associate Director for Administration and Budget (A&B). As the MMS Chief Information Officer, is responsible for ensuring bureau program compliance with applicable laws, regulations, and rules.

B. Chief of Staff (COS) for A&B and Administrative Service Center (ASC) Managers. Responsibilities include, but are not limited to, the following:

(1) Designating qualified individuals to fill the roles of Registrars and Local Issuing Authorities as defined in FIPS-201 for their respective areas of responsibility.

(2) Designating a Facility Physical Access Control Administrator to operate security management software in MMS facilities in their respective areas.

(3) Determining individual physical access rights for the PIV-enabled readers in MMS facilities in their respective areas.

(4) Reviewing and approving requests to review data contained in their facilities' security management software in compliance with the guidelines set forth in Section 14 of this IPD.

(5) Safeguarding data contained in the facility security management software in their respective areas of responsibility from unauthorized disclosure.

(6) Ensuring that a Privacy Act briefing is provided to designated Registrars, Local Issuing Authorities, and the Physical Access Control Administrators.

C. Bureau Security Officer (BSO). Responsibilities include, but are not limited to, the following:

(1) Local Issuing Authority for MMS Headquarters.

(2) Processing and adjudicating NAC and background investigations for MMS and other agencies under the terms of a reimbursable service agreement.

(3) Timely notification to the DOI 24-hour Watch Office of lost or stolen PIV credentials.

(4) Performing the identity proofing and accrediting of the bureau designated Registrars and Local Issuing Authorities in accordance with FIPS-201.

(5) Safeguarding personal information collected during the process from unauthorized disclosure in accordance with the Privacy Act.

(6) Conducting periodic reviews of MMS PIV credential-issuing activities to ensure that bureau security, privacy, and accountability procedures are in compliance with the HSPD-12 and FIPS-201 Directives.

(7) Conducting periodic inspections of physical access control audits at MMS facilities and for initiating appropriate actions in response to unresolved failed entry attempts, other unusual records, or any discrepancies noted.

D. Sponsor. Typically, a sponsor is a manager or supervisor for a Federal employee or other authorized individual or a Contract Officer's Technical Representative (COTR) for a contract applicant. Responsibilities include, but are not limited to the following:

(1) Substantiating the need and initiating the PIV Request Form.

(2) Ascertaining the appropriate risk level designation for the position to be encumbered by the Applicant based on determining criteria contained in Part 441 of the Department Manual, Chapter 3.

(3) Safeguarding personal information collected during the process from unauthorized disclosure in accordance with the Privacy Act.

E. Registrar. The position is filled by Federal employees in the Servicing Human Resources (HR) Office or other office as designated by the COS for A&B or ASC Manager. Responsibilities include, but are not limited to, the following:

(1) Successfully completing the web-based training and certification process on the duties and responsibilities of the role.

(2) Performing the identity-proofing process on an Applicant in accordance with the provisions of FIPS-201.

(3) Fingerprinting the Applicant in accordance with the provisions of FIPS-201.

(4) Completing the PIV Registration Form as required of the role.

(5) Maintaining at least a low risk background investigation.

(6) Safeguarding personal information collected during the process from unauthorized disclosure in accordance with the Privacy Act.

F. Local Issuing Authority. The position is filled by Federal employees and designated by the COS for A&B and the ASC Managers. Responsibilities include, but are not limited to, the following:

(1) Successfully completing the web-based training and certification process on the duties and responsibilities of the role.

(2) Issuing the PIV credential to an Applicant following the positive completion of all identity proofing, background checks, and related approvals.

(3) Completing the PIV Registration Form as required of the role.

(4) Successfully completing the training and certification process in the web-based training on the duties and responsibilities of the role.

(5) Immediately notifying the BSO of a lost or stolen PIV credential.

(6) Maintaining at least a low-risk background investigation.

(7) Safeguarding personal information collected during the process from unauthorized disclosure in accordance with the Privacy Act.

G. Applicant. Responsibilities include, but are not limited to, the following:

(1) Completing the PIV Registration Form as required.

(2) Successfully obtaining and maintaining a background investigation commensurate with the duties and responsibilities of the position that they encumber.

(3) Safeguarding their issued PIV credentials.

(4) Immediately notifying the Local Issuing Authority of a lost or stolen PIV credential.

H. Servicing HR Office. Responsibilities include, but are not limited to, issuing a letter tentatively offering employment to the Applicant prior to their scheduled entry on duty date that includes information on the PIV enrollment process, required background investigation, and IT Security Training and IT Rules of Behavior.

I. Procurement Division. Responsibilities include, but are not limited to, the following:

(1) Inserting a provision into all new contracts, including exercised options, requiring contractors having access in excess of 180 calendar days to bureau-controlled information systems and facilities to comply with the provisions of HSPD-12.

(2) Modifying contracts to be in compliance with any Federal Acquisition Regulation changes in respect to HSPD-12.

J. Designated Facility Physical Access Control Administrators. Responsibilities include, but are not limited to, the following:

(1) Loading access rights onto the physical access control cards.

(2) Safeguarding personal information collected during the process from unauthorized disclosure in accordance with the Privacy Act.

(3) Maintaining at least a low risk background investigation.

(4) Generating and reviewing audit logs of the physical access control system at least once every 2 months, with careful consideration of any failed entry attempts or any other unusual records.

(5) Contacting the BSO concerning any unresolved failed entry attempts or other unusual records contained in the audit logs of the physical access control system.

9. Procedures.

A. PIV credentials may be issued to the following except as noted in Section 9B below:

(1) Federal employees of the MMS.

(2) Contract employees of the MMS who are affiliated with MMS in excess of 180 calendar days and require access to bureau-controlled information systems and facilities as defined in Section 6, paragraphs d and e of this IPD.

(3) Other authorized individuals (e.g., interns, guest researchers, tribal users, volunteers, intermittent, temporary, or seasonal employees) who are affiliated with MMS in excess of 180 calendar days and require access to bureau-controlled information systems and facilities as defined in Section 6, paragraphs (d) and (e) of this IPD.

(4) Individuals affiliated with MMS who are granted access to bureau controlled information systems but are not supervised by an individual with an active HSPD-12 identification card, regardless of the duration of access.

(5) Non-U.S. citizens affiliated with MMS who have successfully completed an HSPD-12 compliant background investigations.

B. Supervised physical and logical access will be granted to certain individuals without being issued PIV credentials under the following conditions:

(1) Federal employees, contractors, and other authorized individuals who are affiliated with MMS for 180 calendar days or less. The 180 calendar-day period begins the first day the individual is affiliated with MMS and ends exactly 180 calendar days later, no matter the frequency or duration of the activity (1 or 5 days a week). These individuals are provided limited and controlled access to bureau facilities and information systems. At a minimum, individuals must access the facility through a screening

system, display a temporary/visitor badge at all times, and/or be escorted at all times. The screening system involves presenting for examination an identification issued by a federal, state, or local government agency or entity, provided it contains a photograph or a school identification card with a photograph prior to being issued a temporary/visitor pass. Temporary/visitor cards must be visually and electronically distinguishable from PIV credentials. The card is valid for use in the facility where issued and cannot be used at other offices across MMS or other government agencies (example – a temporary/visitor card issued in Denver is valid in MMS facilities on the Denver Federal Center (DFC) and surrounding area, but is not valid in the New Orleans area facilities or the Herndon facility).

(2) Contracts and agreements that require non-MMS personnel to access bureau-controlled information systems require supervision (by an individual with a valid PIV credential) or PIV credential for all individuals working in support of the contract/agreement, even those working for 180 calendar days or less.

(3) Vendors, delivery services, recurring services contracts, or other individuals who do not access MMS-controlled information systems but require sporadic physical access in excess of 180 calendar days must access the facility through a screening system, display a temporary/visitor badge at all times, and/or be escorted at all times. The screening system involves presenting for examination an identification issued by a federal, state, or local government agency or entity provided it contains a photograph or a school identification card with a photograph prior to being issued a temporary/visitor pass. Temporary/visitor cards must be visually and electronically distinguishable from PIV credentials. The card is valid for use in the facility where issued and cannot be used at other offices across MMS or other government agencies (example – a temporary/visitor card issued in Denver is valid in MMS facilities on the DFC and surrounding area, but is not valid in the New Orleans area facilities or the Herndon facility).

(4) If at any time a risk-based analysis determines that a PIV credential is warranted for a particular individual or facility, all exceptions listed in Section 9B of this IPD will be immediately rescinded.

(5) Applicability of these standards to Federal employees, contractors, or other authorized individuals accessing bureau-controlled information systems from a non-MMS facility (e.g., researchers up-loading data through a secure website or a contractor accessing bureau-controlled systems from their own facility) should be based on risk. Minimum acceptable requirements for individuals accessing bureau information systems are defined in Section 9A, paragraphs (1) – (4) and Section 9B, paragraphs (1) – (3) of this IPD.

(6) Educational institutions that meet the definition of an MMS-controlled facility and/or enjoy access to bureau-controlled information systems must meet the standards set forth in HSPD-12 and this IPD. Unless specifically designated, the provisions of this IPD do not apply to educational institutions that conduct activities on behalf of MMS, or where MMS employees are hosted.

C. For purposes of background investigations, contractors and contractor employees acting for or on behalf of MMS must obtain, and maintain, a favorably adjudicated background investigation at a level equal to that which would be conducted for a Federal employee with similar duties and responsibilities.

D. All new contracts, including exercised options, requiring contractors to have long-term access (excess of 180 calendar days) to bureau-controlled information systems and facilities must include a requirement to comply with the HSPD-12 Directive for affected contractor personnel. The MMS contracts must also be modified to be in compliance with any Federal Acquisition Regulation changes in respect to these requirements.

E. Federal employees, contractors, and other authorized individuals who require unsupervised access to bureau-controlled information systems and facilities will be issued PIV credentials only after an appropriate background investigation and NAC has been favorably adjudicated. An Applicant awaiting the results of a NAC, those affiliated with MMS for 180 calendar days or less, and visitors will have limited and controlled access to the facility via a screening system, display a temporary/visitor badge at all times, and/or be escorted at all times. The screening system involves presenting for examination an identification issued by a federal, state, or local government agency or entity, provided it contains a photograph or a school identification card with a photograph prior to being issued a temporary/visitor pass. Temporary/visitor cards must be visually and electronically distinguishable from PIV credentials. The card is valid for use in the facility where issued and cannot be used at other offices across MMS or other government agencies (example – a temporary/visitor card issued in Denver is valid in MMS facilities at the Denver Federal Center and surrounding area, but is not valid in the New Orleans area facilities or the Herndon facility).

F. In the event that a credential is lost or stolen, the cardholder must immediately notify the Local Issuing Authority.

10. Milestones.

A. HSPD-12 PIV Compliant Credentials.

(1) MMS employees, applicants, contractors, and other authorized individuals entering on duty on or after October 27, 2005, must comply with the provisions of HSPD-12.

(2) MMS employees, applicants, contractors, and other authorized individuals entering on duty after October 27, 2006, are required to be issued PIV credentials. Additionally by this date, all PIV credentials issued by departments and agencies will be interoperable across federal domains.

(3) MMS employees, applicants, contractors, and other authorized individuals who have entered on duty prior to October 27, 2005, have until October 27, 2007, to comply with the provisions of HSPD-12 and to be issued PIV credentials.

B. Background Investigations. MMS employees with background investigations on file that are over 15 years old must have a re-investigation completed and favorably adjudicated by October 27, 2008. The scope of the investigation must be at a level commensurate with the duties and responsibilities of the position that they encumber.

11. Issuing Process. FIPS-201 requires the adoption and use of an approved identity proofing and registration process. The MMS will employ a hybrid of the FIPS-201 designed role-based and system-based models for issuing PIV credentials. Under this model, one person cannot perform more than one

role in the process. This is designed to safeguard against the possibility of collusion between the Applicant (as identified below) and one of the other roles. The credential can only be issued by providers whose reliability has been established by an official accreditation process. Training and certification in the duties and responsibilities of each role is required and is available in a web-based format. Personnel to fill the roles of Registrars and Local Issuing Authorities (as identified below) are designated by the COS for A&B or the ASC Managers as applicable, and must be Federal employees with at least a current low risk background investigation.

A. The MMS Role-Based Model.

(1) Applicant is a tentatively selected MMS job applicant, contractor, or other authorized individual with a need to be issued a PIV credential.

(2) Sponsor substantiates the need for a PIV credential to be issued to an Applicant and forwards the request to the Registrar. The Sponsor is typically a manager/supervisor for an MMS employee and/or other authorized individual or a COTR for a contract applicant. The Sponsor ascertains the appropriate risk level designation for the position based on determining criteria found in the Departmental Manual 441 DM 3. Once the risk level designation has been determined the Registrar or another HR representative will advise the Sponsor of the type of background investigation needed and the required forms.

(3) Registrar is the Servicing HR Office (or other office as designated by the COS for A&B or ASC Managers) who performs the identity proofing.

(4) Local Issuing Authority for MMS Headquarters is the Bureau Security Officer. The ASCs, Satellite Offices, and Program Field Offices will have Local Issuing Authorities designated by the ASC Managers.

B. Identity-Proofing and Registration Process Steps.

(1) Sponsor is typically a manager/supervisor for an MMS employee and/or other authorized individual or a COTR for a contract Applicant.

(a) When a new MMS employee or contractor is selected, the Sponsor initiates the process by completing Section A of the PIV Request Form. All information on the form must be legibly printed in blue or black ink. Strikethroughs must be initialed and forms with white-out will not be accepted. All signatures must be original signatures, no copies or stamped signatures will be accepted. Once the Sponsor signs the form, it should never be provided to the Applicant except to complete information in the presence of the Registrar or Local Issuing Authority.

(b) The Sponsor is responsible for ascertaining the appropriate risk level designation for the position based on determining criteria found in 441 DM 3. Once the risk level designation has been determined, the Registrar or another HR representative will advise the Sponsor of the type of background investigation needed and the required forms.

The background investigation forms are included in the letter tentatively offering employment issued

by the Servicing HR Office to the Applicant (Federal employee or other authorized individual). The letter issued by the Servicing HR Office instructs the Applicant to report for initial PIV processing (fingerprinting) and to submit their completed background investigation forms. The Applicant must bring with him two forms of identity source documents, one of which must be an identification issued by a federal, state, or local government agency or entity provided it contains a photograph or a school identification card with a photograph. The documents must meet the standards contained in I-9, OMB No. 1115-0136, Employment Eligibility.

In the case of contractors, the Applicant receives the forms directly from the COTR. The COTR is responsible for arranging the initial PIV processing for the contract Applicant with the Servicing HR Office. The identity proofing procedures requirements outlined above also apply to the contractor Applicant.

The background investigation requirement may be satisfied by locating and referencing a completed and favorably adjudicated investigation. Therefore, Applicants with a valid background investigation on file at a level commensurate with the duties and responsibilities of the position that they will encumber may not require an additional background check. The PIV Request Form is still required. However the identity proofing procedure can take place at the time of entry on duty. Contact the BSO for the background investigation status of employees transferring from other Federal agencies and contractors.

(2) Registrar is the Servicing HR Office (or other office as designated by the COS or ASC Managers).

(a) Receives the completed background investigation forms from the Applicant and the PIV Request Form from the Sponsor.

(b) The Applicant presents two identity source documents to the Registrar who conducts the identity proofing procedure. The Registrar reviews the documents to ensure, to the best of his ability, that the documents are authentic and have not been altered. A copy of the documents is made.

(c) Takes a full set of fingerprints from the Applicant.

(d) Completes Section B of the PIV Request Form with the exception of #32-35 which are completed by the BSO.

(e) Forwards the completed background investigation forms, fingerprints, copies of the two identity source documents, and the PIV Request Form to the BSO.

(f) At the time of entry on duty, the Applicant appears before the Registrar and must successfully complete the DOI IT Security Awareness Training course online. Additionally, the Applicant is provided a copy of the MMS IT Rules of Behavior and must sign a certificate acknowledging that they have been informed of their responsibilities for safeguarding MMS IT resources. The IT Rules of Behavior certificate is then sent by the Registrar to the Bureau Information Technology Security Manager. Also at this time, the I-9 Identification Verification Form is completed and forwarded to the BSO for retention. This form is not required for contractor Applicants.

(2) The BSO.

(a) Initiates the appropriate background investigation to include a NAC through OPM. The results of the NAC are generally available 10 – 14 business days from the date OPM receives the forms and schedules the investigation.

(b) Adjudicates the NAC and notifies the Registrar and the Local Issuing Authority that the results are favorable. If the results are unfavorable, the Applicant will not be issued a PIV credential. If the results of the full background investigation are unfavorable, the BSO will notify the Local Issuing Authority to immediately revoke the Applicant's PIV credential. Existing appeal processes are available through the BSO.

(c) Completes Section B, #32-35 of the PIV Request Form and forwards the form and copies of the identity source documents to the Registrar.

(d) Once the PIV credential issuing process is completed, the original I-9 Identification Verification Form (Federal employees only), PIV Request Form, and the copies of the identity source documents are forwarded to the BSO for retention in accordance with the provisions of the Privacy Act.

(3) Local Issuing Authority. The MMS Headquarters Local Issuing Authority is the BSO. The ASC, Satellite Offices, and Program Field Offices will have Local Issuing Authorities designated by the ASC Managers.

(a) At the time of entry on duty the Local Issuing Authority receives the PIV Request Form and copies of the identity source documents from the Registrar. The Applicant appears in person before the Local Issuing Authority to collect the PIV credential. The Local Issuing Authority completes the chain of trust by performing a 1:1 biometric inspection of the Applicant (a comparison of the Applicant's facial features against the photo identification provided during the initial PIV processing fulfills this requirement). After confirming the Applicant's identity, the Local Issuing Authority completes the DI-238 or DI-238A (as applicable) Identification Card. A digital facial image of the Applicant is taken and placed on the identification card. A copy of the image is stored in a jpg format that can be transferred by e-mail.

(b) Completes Section C of the PIV Request Form.

(c) Obtains the Applicant's signature on the PIV Request Form, Section D.

(d) Provides the Applicant the completed DI-238 or DI-238A as applicable.

(e) Issues the Applicant a physical access control card, as applicable.

(f) Forwards the completed PIV Request Form and the copies of the two identity source documents to the BSO for record retention.

12. Card Renewal, Reissue, Suspension, Revocation, and Destruction.

A. Card renewal replaces an expired card, repeating the identity proofing and registration process. Card renewal requires the following:

(1) A completed PIV Request Form.

(2) An updated digital facial image of the Applicant.

(3) Local Issuing Authority collects and destroys the expired card.

B. Reissue occurs when a PIV credential has been lost or stolen. Reissue requires the following:

(1) A completed PIV Request Form.

(2) An updated digital facial image of the Applicant.

C. Certain circumstances require a PIV credential to be suspended. Commonly such suspensions are temporary (for example, military or medical leave in excess of 12 consecutive months). Card suspension requires the Local Issuing Authority to perform the following:

(1) Collect and store the PIV credential in a secure location.

(2) If the individual has been away in excess of 12 consecutive months and their card has remained in a suspended status, reissue a new PIV credential following the procedures outlined in Section 11A.

(3) Coordinate with the Supervisor/Manager or COTR to complete the Exit Clearance Process if applicable.

D. Revocation of a PIV credential is necessary when the card has been compromised (i.e., stolen or lost) or when the cardholder is separated from the MMS. Card revocation requires the Local Issuing Authority to perform the following:

(1) If available, destroy the card.

(2) Coordinate with the Supervisor/Manager or COTR to complete the Exit Clearance Process if applicable.

(3) If the PIV credential has been lost or stolen, follow the established procedures as outlined in Section 11A for replacement.

E. Repetitive Losses.

(1) First reported loss – Local Issuing Authority follows established procedures for lost/stolen card.

(2) Second reported loss – Local Issuing Authority follows established procedures for lost/stolen card.

(3) Three or more lost cards – Local Issuing Authority follows established procedures for lost/stolen card and reports the incident to the Program Office for appropriate action that may include discipline.

F. Temporary/Visitor Cards.

(1) When an individual requires a replacement credential, the temporary/visitor card will be issued by the Local Issuing Authority in accordance with Section 11A or 11B as applicable.

(2) Temporary/visitor cards are visually distinguishable from PIV credentials. The card is valid for use in the facility where issued and cannot be used at other offices across the MMS or other government agencies (example – a temporary/visitor card issued in Denver is valid in MMS facilities at the Denver Federal Center and surrounding area, but is not valid in the New Orleans area facilities or the Herndon facility). Employees, contractors and other authorized individuals are accountable for temporary/visitor cards that they are issued.

G. Collected PIV credentials and PIV credentials intended for destruction should be immediately destroyed.

13. Access Control System. The bureau has elected to transition physical access control systems in all MMS facilities to PIV compliant readers. The PIV credential will become the standard MMS identification card. When fully implemented with PIV-enabled card readers, the credential will provide physical access to MMS facilities and logical access to bureau-controlled information systems. PIV enabled card readers authenticate the PIV credential holder and communicate with the back-end PIV Secure Issue Process Database/Card Management System and the facility's security management software for a physical access control application. The system determines whether or not to grant access based on a predefined set of rules called rights. Access rights specify which readers the credential holder is allowed to use and at what time. The rights are determined and set locally in the facility's security management software loaded on a dedicated server or a client PC that is connected to the server through a network. Designation of a Facility Physical Access Administrator to manage the MMS facility's security management software and assignment of individual rights for the PIV-enabled physical access system will be controlled locally by the COS for A&B or the ASC Managers, as applicable.

Until an MMS facility fully migrates to PIV-enabled readers, policies and procedures governing the current physical access control systems will remain in effect.

14. Privacy Act. Personnel and access information contained in the PIV Registration Process and all MMS facility's security management software is covered by the Interior Department – Privacy Act Notice. The Department has initiated the requisite notifications in accordance with the use, security, and maintenance of personal information collected to facilitate the implementation of this system in compliance with the provisions of the Privacy Act. In accordance with the notice, data such as personal information and access information is not to be disclosed to anyone outside of those listed in the notice. The information contained in all MMS facilities' security management software will routinely be used for physical access control and, in rare circumstances, may be used for time and attendance purposes or other personnel-related matters in limited circumstances. Requests to access such information must be specific and the reasons clearly established. All requests to review

information contained in an MMS facility's security management software must be in writing to the COS for A&B or the ASC Managers, as applicable, for approval.

15. Audits and Controls. The BSO will conduct periodic reviews of MMS PIV credential-issuing activities to ensure that bureau security, privacy, and accountability procedures are compliant with HSPD-12 and FIPS-201 Directives. The BSO is also responsible for conducting periodic inspections of physical access control audits for all MMS facilities. The Physical Access Control Administrators are responsible for generating and reviewing audit logs of the physical access control systems under their respective control at least once every 2 months, with careful consideration of any failed entry attempts or any other unusual records. Any unresolved failed entry attempts or unusual records must be immediately reported to the BSO.

16. Reporting Requirements. Applicants are responsible for safeguarding their issued PIV credential. In the event of a loss or theft, the Local Issuing Authority must be immediately notified and the cardholder must explain the circumstances of the loss. The Local Issuing Authority is responsible for notifying the BSO of a lost or stolen credential as soon as possible. The BSO is then responsible for notifying the DOI 24-hour Watch Office.

17. Cancellation. The IPD will remain in effect until incorporated into the MMS Manual.

Robert E. Brown
Associate Director for
Administration and Budget

Appendix – Acronyms Used in This IPD:

A&B	Administration and Budget
ASC	Administrative Service Center
BSO	Bureau Security Office
COS	Chief of Staff, Administration and Budget
COTR	Contracting Officer's Technical Representative
DOI	Department of the Interior
FedEx	Federal Express
FIPS-201	Federal Information Processing Standards Publication
HR	Servicing Human Resources Office
HSPD-12	Homeland Security Presidential Directive 12
IPD	Interim Policy Document
MMS	Minerals Management Service
NAC	National Agency Check
NBC	National Business Center (Department of the Interior)
NIST	National Institute of Standards
OCIO	Office of the Chief Information Officer (DOI)
OMB	Office of Management and Budget
OPM	Office of Personnel Management
PIN	Personal Identity Number
PIV	Personal Identity Verification
UPS	United Parcel Service
USC	United States Code