

DATE: December 18, 2006

TO: DIRECTIVES POINTS OF CONTACT AND REVIEWERS

FROM: WALTER HOWES, ACTING DIRECTOR
OFFICE OF INFORMATION RESOURCES, MA-44

SUBJECT: REDLINE/STRIKEOUT FOR DRAFT DOE N 206.4, *Personal Identity Verification*

In accordance with Directives procedures, a redline/strikeout of the Order has been posted to RevCom to allow interested parties to see the cumulative effect of changes produced during coordination.

Draft DOE N 206.4 was coordinated in RevCom beginning in November 2006. The directive writer has responded to all comments and incorporated those comments he accepted into the directive. Please go to the following URL to review the redline/strikeout:
<http://www.directives.doe.gov/rcLogin.html>.

Reviewing Instructions:

1. **THIS IS NOT AN OPPORTUNITY TO SUBMIT NEW COMMENTS.**
2. **Only** comments with specific objections to the changes in the Directive will be addressed.
3. Headquarters DPCs have until **January 4, 2007**, to review the redline/strikeout and compile and submit comments/concurrence/nonconcurrence through RevCom.
4. Reviewers in the field are asked to meet assigned internal organizational deadlines and respond as follows:

If you:	Then:
submitted a major comment and agree with the incorporation of your comments	go into RevCom and concur.
submitted a major comment and do not agree with the incorporation of your comments	go into RevCom, nonconcur, and submit justification for your nonconcurrence.
did not comment, but the incorporation of others' comments may have an adverse impact on your organization's mission	go into RevCom and explain how this directive will adversely impact your organization's mission.
did not comment, and are still satisfied with the directive	no action is necessary

SUBJECT: PERSONAL IDENTITY VERIFICATION

1. **OBJECTIVE.** To implement the requirements of Homeland Security Presidential Directive 12 (HSPD-12) related to the secure and reliable identification of Department of Energy (DOE) Federal and contractor employees. In particular, this Notice concerns the objective of HSPD-12, which requires such identification to be issued based upon sound criteria for verifying an individual's identity. HSPD-12 requirements are being instituted incrementally within DOE beginning with the incorporation of HSPD-12 identity proofing procedures into the current issuance process for DOE security badges.

During the initial implementation of HSPD-12 the Department is required to issue a Federal agency identity credential which will indicate that an individual's identity has been verified through the HSPD-12 personal identity verification (PIV) process. The DOE security badge identified in DOE M 470.4-2, *Physical Protection*, Chapter XV, paragraph 2a, "DOE Federal and Contractor Employee Badges," has been determined to be the Department's Federal agency identity credential. This badge will be issued to Federal employees and contractor employees designated by the Secretary of Energy and additional contractor employees as determined by the applicable Departmental element. The local site specific access badge, temporary visitor badge, Office of Science badge, and foreign national badge are not HSPD-12 compliant and are not recognized as the Department's Federal agency identity credential.

2. **CANCELLATION.** DOE N 206.3, *Personal Identity Verification*, dated 11-22-05. Cancellation of a Notice does not, by itself, modify or otherwise affect any contractual obligation to comply with the Notice. Contractor requirements documents (CRDs) that have been incorporated into or attached to a contract remain in effect until the contract is modified to either eliminate requirements that are no longer applicable or substitute a new set of requirements.
3. **APPLICABILITY.**
 - a. **All Departmental Elements.** Except for the exclusion in paragraph 3c, this Notice applies to all DOE Federal employees, contractor employees and applicants for employment within all Departmental elements who require a DOE security badge. (See a complete list of DOE elements online at <http://www.directives.doe.gov/pdfs/reftools/org-list.pdf>. This list automatically includes Departmental elements created after the Notice is issued.) Mandatory applicability of this Notice is determined by the Secretary of Energy. Additional applicability may be determined by the responsible Departmental element. This Notice automatically applies to Departmental elements created after it is issued. This Notice does apply to those facilities that do not currently issue badges.

The National Nuclear Security Administration (NNSA) Administrator will assure that NNSA employees and contractors comply with their respective responsibilities under this Notice. Nothing in this Notice will be construed to interfere with the NNSA Administrator's authority under Section 3212 (d) of Public Law (P.L.) 106-65 to establish Administration-specific policies, unless disapproved by the Secretary.

- b. DOE Contractors. Except for the exclusion in paragraph 3c, the Contractor Requirements Document (CRD), Attachment 1, sets forth requirements of this Notice that will apply to contracts that include the CRD. The CRD must be included in contracts that include responsibility for physical access to a DOE-owned or DOE-leased facility.
- c. Exclusion. In accordance with the responsibilities and authorities assigned by Executive Order (E.O.) 12344 and to ensure consistency throughout the joint Navy and DOE organization of the Naval Nuclear Propulsion Program, the Director of the Naval Nuclear Propulsion Program will implement and oversee all requirements and practices pertaining to this DOE Notice for activities under the Director's cognizance.

4. REQUIREMENTS.

- a. General.
 - (1) Security badges can only be issued to individuals whose identity has been verified via—
 - (a) presentation of two original identity source documents and
 - (b) a background investigation (BI).
 - (2) No individual known or suspected by the government of being a terrorist may be issued a security badge.
 - (3) Expired or invalidated security badges must be immediately revoked and confiscated.
 - (4) The security badge described in DOE M 470.4-2, *Physical Protection*, dated 8-26-05, Chapter XV, currently serves as the identification credential required by HSPD-12.
 - (5) Foreign National employees/contractors/visitors will be processed in accordance with DOE O 142.1, *Classified Visits Involving Foreign Nationals*, dated 1-13-04, and DOE O 142.3, *Unclassified Foreign Visits and Assignments Program*, dated 6-18-04, pending further Office of Management and Budget guidance.

- (6) Individuals who do not require a DOE security badge, including short term (6 consecutive months or less) uncleared contractors, but require access to DOE facilities are issued badges consistent with Departmental policies and local procedures. For short-term individuals, at a minimum, the following procedures will be implemented.
 - (a) Apply adequate controls to systems and facilities (i.e., ensuring short-term individuals have limited/controlled access to facilities).
 - (b) Provide short-term individuals with clear documentation on the rules of behavior and consequences for failure to comply before granting access to facilities and/or systems.
 - (c) The badges issued to these short-term individuals must be visually distinguishable from security badges issued to individuals to whom Federal Information Processing Standards (FIPS) Publication (Pub) 201 does apply.
- (7) Heads of Departmental and field elements are responsible for ensuring that managers of sites under their cognizance responsible for identity proofing complete the Accreditation Checklist (Attachment 2).¹ The completed checklist is to be provided to the Office of the Chief Information Officer. No new DOE security badge can be issued by any site until the self-accreditation is positively completed and sent to the Office of the Chief Information Officer.
- (8) Heads of Departmental and field elements are responsible for ensuring that personal information collected for employee and contractor identification is handled in accordance with the Privacy Act of 1974.

b. Procedures.

- (1) The procedures below apply to DOE Federal employees and applicants for employment who will require access to DOE-owned and DOE-leased facilities in the performance of official duties. The identity proofing procedures also apply to individuals who will be issued a security badge and are DOE contractor employees and applicants for employment with them, as delineated in the CRD (Attachment 1).
- (2) Specific roles for executing these procedures are defined under paragraph 6, "Definitions," below. The roles of applicant, sponsor, registrar, and issuer are mutually exclusive; one individual must not hold

¹Sites that will not issue DOE security badges may complete the Accreditation Checklist by returning the Checklist with negative responses and a statement that the site will not issue DOE security badges.

more than one of these roles in the identity proofing process. (Note: For DOE Headquarters, the role of registrar will be fulfilled by the Office of Personnel Security.)

- (3) The sponsor requests a security badge for the applicant. The request, which is sent to the registrar, must include the following information:
 - (a) sponsor name, organization, and contact information, including the address of the sponsoring organization;
 - (b) applicant name, date of birth, position, and contact information;
 - (c) registrar name and contact information;
 - (d) issuer name and contact information; and
 - (e) sponsor signature.
- (4) The applicant completes BI forms as required for a Federal employment suitability investigation or a personnel security investigation, if the applicant will require access authorization under DOE M 470.4-5, *Personnel Security*, dated 8-26-05, and submits to the registrar.
- (5) If the applicant is currently awaiting a hearing or trial; has been convicted of a crime punishable by imprisonment of 6 months or longer; or is awaiting or serving a form of pre-prosecution probation, suspended or deferred sentencing, probation, or parole in conjunction with an arrest or criminal charges against the individual for a crime that is punishable by imprisonment of 6 months or longer, the registrar may suspend further processing and notify the sponsor of the cause. At such time as the hearing, trial, criminal prosecution, suspended sentencing, deferred sentencing, probation, or parole has been completed, the applicant may be resubmitted to the identity proofing process to determine eligibility for a DOE security badge permitting unescorted access to DOE facilities.
- (6) The applicant appears in person before the registrar or registrar designee (Federal or contractor employee) with two identity source documents in original form. If applicants are physically remote from the registrar, the head of the Departmental element or field element having cognizance over the identity proofing process must designate, in writing, an individual located in proximity to the applicant to act as registrar by proxy. Identity source documents must come from the list of acceptable documents included in Form I-9, OMB No. 1115-0136, *Employment Eligibility Verification*. At least one of the documents must be a valid State- or

Federal Government-issued picture identification (see <http://www.uscis.gov/files/form/i-9.pdf>).

Deleted:
<http://www.uscis.gov/graphics/formsfee/forms/files/i-9.pdf>
Formatted: Default Paragraph Font

- (7) The registrar or registrar designee validates the applicant’s identity and source documents and makes a record copy for each identity source document consisting of—
 - (a) document title,
 - (b) document issuing authority,
 - (c) document number,
 - (d) document expiration date (if any), and
 - (e) any other information used to confirm the identity of the applicant.

- (8) The registrar—
 - (a) compares the applicant’s information with information on the sponsor’s request;
 - (b) has the applicant’s photograph taken;
 - (c) checks for a prior BI,² either from previous Federal employment or a previous position requiring an access authorization/personnel security clearance;
 - (d) has the applicant’s fingerprints taken for the BI request package; and
 - (e) retains a copy of fingerprint data and identity source validation documentation in a file created and maintained specifically for identity proofing records. [NOTE: When identity proofing is linked to a personnel security determination, the personnel security file (PSF) is only used for documentation of the personnel security process, not documentation related solely to the identity proofing process.]

- (9) The registrar submits the BI request packages as follows.
(Note: The Registrar only needs to submit a BI request package if an acceptable prior BI cannot be verified.)

Formatted: Space After: 0 pt

Deleted: through a check of

Deleted: can

Deleted: Request for Preliminary Employment Data (SF

Deleted: -

Deleted: 75),

Inserted:

Deleted: -

²Record of a prior investigation may be found in the Central Personnel Clearance Index (CPCI) database, Request for Preliminary Employment Data (SF 75), or other means. Indication of prior investigation may be found on an applicant’s Questionnaire for Public Trust Positions (SF 85P), or Questionnaire for National Security Positions (SF 86), where these forms are used.

- (a) For applicants not requiring access authorization (personnel security clearance), the registrar submits requests to the Office of Personnel Management (OPM) using the appropriate OPM submitting office number (SON) for the servicing personnel office.
- (b) For applicants requiring access authorization, the registrar submits packages to the processing personnel security office.
- (c) All BI submissions must include a request for an advance National Agency Check (NAC).

(10) When the BI, or any part thereof, including the FBI criminal history fingerprint portion is received, it, or a copy, will be forwarded to the registrar for adjudication. In the adjudication process, the registrar shall have the authority to obtain additional information as may be deemed necessary to resolve possible issues of concern pertaining to the applicant. The following are disqualifying criteria but are not all inclusive and may vary depending on access requirements:

Deleted: PIV

- (a) The individual is, or is suspected of being, a terrorist.
- (b) There is an outstanding warrant against the individual.
- (c) The individual has deliberately omitted, concealed, or falsified relevant and material facts from any *Questionnaire for National Security Positions* (SF 86), *Questionnaire for Non-Sensitive Positions* (SF 85), or similar form used in the determination of eligibility for a DOE security badge.
- (d) The individual has presented false or forged identity source documents.
- (e) The individual has been barred from Federal employment.

Deleted: -

Deleted: -

(11) Once eligibility for a DOE security badge has been determined, the badge is issued in accordance with the following. [Note: A DOE security badge can be issued based upon favorable results from the FBI National Criminal History Check (fingerprint check).]

- (a) The registrar signs indicating approval and sends notification of favorable determination of eligibility for unescorted access to DOE facilities, the applicant's photograph, and other data associated with the applicant to the badge issuing office (issuer). This information should be handled in accordance with the requirements of DOE M 471.3-1, *Identifying and Protecting for Official Use Only Information*, Chapter II, paragraph 2e.

Deleted: via secure means.

- (b) The issuer ascertains the completeness of the information provided by the registrar, including the fact of a favorable adjudication, and creates a DOE security badge.
 - (c) The applicant signs for and collects the security badge in person at the badge office (or at an office authorized to act as issuer) by presenting a valid State- or Federal Government-issued picture identity source document. The issuer validates the appearance of the applicant against the photograph on the identity source document and validates the name and photograph of the security badge against those on the identity source document.
 - (d) All documentation created in the security badging process will be retained in an identity-proofing file created for the individual applicant and given a unique file identification.
 - (e) If, subsequent to the issuance of the security badge, further processing of the BI by the registrar reveals derogatory information to be adjudicated under the criteria established in 4(b)(10) above, DOE access privileges will be immediately reviewed and in accordance with current security procedures, site security and human resources management will:
 - 1 Determine the level of continued DOE access privileges and whether the security badge will be recovered, and
 - 2 Based on the resolution of the PIV adjudication and/or appeals process, either revoke or reinstate DOE badge and access privileges as appropriate.
- (12) For unfavorable adjudication under the criteria in paragraph 4(b)(10) above, the registrar must do the following within 2 working days of the determination:
- (a) notify the sponsor in writing that a DOE security badge will not be issued to the applicant;
 - (b) notify the applicant in writing of the unfavorable adjudication [the notification must contain the reasons for the denial of the DOE security badge and the appeal process available to the applicant as detailed in paragraph 4(b)(13), including contact information]; and
 - (c) for those cases with ongoing suitability or personnel security adjudication, maintain contact with the adjudicating office to ensure that final decision information is conveyed to the registrar.

(13) Appeals Process.

(a) The identity proofing appeals process does not supersede, ~~or in any~~ way affect a final determination of eligibility for Federal employment under Title 5, Code of Federal Regulations (CFR), Part 731, or a final determination for eligibility for access to classified matter or special nuclear material as detailed in Title 10, CFR, Part 710.

Deleted: supplant,

(b) Upon receipt of the registrar's denial of badge notice, the applicant has 10 working days in which to indicate, in writing or by electronic means, the intent to file an appeal. The applicant may be represented and advised by counsel or a representative of the applicant's choosing in the appeals process, at the applicant's expense.

(c) The applicant must file the actual appeal 10 working days after notifying the registrar of intent to file. The appeal must be in writing and provide a response to the information that formed the basis of the denial of security badge.

(d) Upon receiving the applicant's notification of intent to file an appeal, the registrar will identify and notify members of the appeals panel. The appeals panel will consist of three members, who must be DOE employees, as follows.

1 A representative of the Departmental or field element having cognizance over the site, appointed by the head of that element, will be the first member of the appeals panel. Such person must be a professional who holds a DOE Q access authorization.

2 A DOE attorney designated by the General Counsel will be the second member of the appeals panel. Such person must hold a DOE Q access authorization.

3 A representative of the security office for the hiring site, appointed by the head of the relevant Departmental or field element, will be designated to act as the third member of the appeals panel. Such person must be a professional who holds a DOE Q access authorization.

(e) Upon receipt of the applicant's written appeal, the registrar prepares an appeals package for each panel member consisting of a copy of all identity proofing documentation maintained by the

registrar, the BI, the notification of denial of security badge providing the registrar's rationale for denial, and the written appeal of the applicant.

- (f) Each panel member will review the package and, within 30 days, respond to the registrar in writing indicating either concurrence or nonconcurrence with the denial of security badge decision. For any nonconcurrence, the panel member will provide a brief rationale.
- (g) The decision of the appeals panel will be determined by simple majority of concurrence or nonconcurrence. This decision is final. The registrar will inform the applicant and sponsor of the appeal decision and, in those instances where there is majority nonconcurrence with denial of security badge, the registrar will follow the steps in paragraph 4(b)(11), above.

5. RESPONSIBILITIES.

a. Office of the Secretary. Provides guidance to the heads of Departmental elements on the application of HSPD-12 and its associated processes requirements for contractors within the Department.

Deleted: p

b. Heads of Departmental Elements.

- (1) Oversee the implementation of this Notice for sites and operations under their immediate cognizance, including assigning tasks and roles to the appropriate site personnel. This includes designation of registrar and issuer and the appointment of members to the appeals panel.
- (2) Ensure contracts affected by this Notice are modified, as appropriate, including ensuring the incorporation of the CRD into contracts in accordance with paragraph 3b of this Notice.
- (3) Verify that any security badging operations under their cognizance observe the requirements of this Notice, thereby establishing that those operations meet approved identity proofing, registration, and security badge issuance procedures under HSPD-12. Verification will be accomplished through the completion of the "Accreditation Checklist" (Attachment 2) by sites under their cognizance.
- (4) For sites under their cognizance, designate the adjudication office for the identity proofing of contractor employees not requiring access authorization.

- (5) For sites under their cognizance, determine which, if any, contractors without access authorizations require an HSPD-12 compliant DOE security badge. The determination should be based on job duties, a risk analysis, and be consistent with DOE security policies.

c. Heads of Field Elements.

- (1) Oversee the implementation of this Notice for sites and operations under their immediate cognizance, including assigning tasks and roles to the appropriate site personnel. This includes designation of registrar and issuer and the appointment of members to the appeals panel.
- (2) Ensure contracts affected by this Notice are modified, as appropriate, including ensuring the incorporation of the CRD into contracts in accordance with paragraph 3b of this Notice.
- (3) Verify that any security badging operations under their cognizance observe the requirements of this Notice, thereby establishing that those operations meet approved identity proofing, registration, and security badge issuance procedures under HSPD-12. Verification will be accomplished through the completion of the “Accreditation Checklist” (Attachment 2) by sites under their cognizance.
- (4) For sites under their cognizance, designate the adjudication office for the identity proofing of contractor employees not requiring access authorization.

d. General Counsel.

- (1) Provides resources for legal advice and assistance regarding revisions to laws and regulations that may affect the implementation of FIPS.
- (2) Provides legal advice and assistance on the privacy implications and effects of the requirements of this Notice and any related Policy developed in response to HSPD-12.

e. Chief Health, Safety and Security Officer, Office of Health, Safety and Security.

Acts as the senior Departmental official responsible for the direction and administration of the DOE Safeguards and Security Program, including promulgation of policy for Departmental personnel security activities and Departmental security badge standards.

Deleted:

f. Director, Office of Procurement and Assistance Management. Develops any necessary HSPD-12 identity proofing guidance for implementation of this Notice in DOE contracts involving physical access to DOE-owned or DOE-leased

facilities, in addition to those in which the CRD has been incorporated in accordance with paragraph 3b of this Notice.

g. Contracting Officers.

- (1) Incorporate the CRD (Attachment 1) into contracts in accordance with paragraph 3b of this Notice.
- (2) Follow any HSPD-12 identity proofing guidance issued by the Director, Office of Procurement and Assistance Management, for any other contracts involving physical access to DOE-owned or DOE-leased facilities.

h. Chief Information Officer.

- (1) Administers and oversees DOE implementation of the Federal information technology laws and regulations, including FIPS applicable to the Department's federally controlled information systems.
- (2) Assembles and reviews completed Accreditation Checklists (Attachment 2) to ensure compliance with FIPS Pub 201.

6. DEFINITIONS.

- a. Applicant. An individual applying for a DOE security badge. The applicant may be a current or prospective Federal hire or a Federal employee or an applicant for employment with a DOE contractor or a current DOE contractor employee.
- b. Employee. Except as otherwise provided by Title 5 U.S.C., section 2105, Chapter 21, Part III, subsection a, an officer or an individual who is (1) appointed in the civil service by one of the individuals listed in this subsection, (2) engaged in the performance of a Federal function under the authority of law or an Executive act, and (3) subject to the supervision of an individual named under this subsection while engaged in the performance of the duties of the position.
- c. Issuer. The organization that is issuing the security badge to an applicant. The badge may be issued by a Federal or contractor employee.
- d. Registrar. The entity that establishes and vouches for the identity of an applicant to an issuer. The registrar authenticates the applicant's identity by verifying identity source documents and adjudicating a BI. The registrar will be a Federal employee and will be appointed by the head of the Departmental/field element in writing.

Deleted: , or registrar proxy,

- e. Registrar by Proxy. An additional federal employee appointed by the head of the Departmental/field element in writing to fulfill all registrar duties in a designated area.
- f. Registrar Designee. The registrar designee may be a federal or contractor employee assigned and designated by the registrar to perform only limited registrar functions, such as verifying I-9 documents, as designated by the registrar.
- g. Security Badge. A distinctive tag used for controlling access to facilities and security areas that provides an individual's name, photograph, and access authorization type and may include additional information in electromagnetic, optical, or other form.
- h. Sponsor. The individual who substantiates the need for a DOE security badge to be issued to the applicant and submits the request to the registrar. The sponsor may be a Federal employee or a DOE authorized major facilities contractor.

Deleted: M&O

7. REFERENCES.

- a. Homeland Security Presidential Directive 12, *Policy for a Common Identification Standard for Federal Employees and Contractors*, dated August 27, 2004, which establishes a mandatory, Government-wide policy for secure and reliable forms of identification issued by the Federal Government to its employees and contractors (see <http://csrc.nist.gov/policies/Presidential-Directive-Hspd-12.html>).
- b. P.L. 99-603 (8 USC 1324a), *Immigration Reform and Control Act of 1986*, which authorizes collection of information on the Form I-9, OMB No. 1115-0136 (see <http://www4.law.cornell.edu/uscode/>).
- c. Federal Information Processing Standards Publication 201, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, dated February 25, 2005, which defines a reliable, government-wide PIV system for use in applications such as access to federally controlled facilities and information systems (see <http://www.csrc.nist.gov/publications/fips/fips201/FIPS-201-022505.pdf>).
- d. Title 5, CFR, Part 731, *Suitability*, which establishes criteria and procedures for making determinations of suitability for employment in positions in the competitive service and for career appointment in the Senior Executive Service (see <http://cfr.law.cornell.edu/cfr/>).
- e. Title 5, CFR, Part 732, *National Security Positions*, which sets forth certain requirements and procedures which each Agency shall observe for determining national security positions (see <http://cfr.law.cornell.edu/cfr/>).

- f. Title 10, CFR, Part 710, *Criteria and Procedures for Determining Eligibility for Access to Classified Matter and Special Nuclear Material*, which establishes the criteria, procedures, and methods for resolving questions concerning the eligibility of individuals who are employed by, or applicants for employment with, Department of Energy contractors, agents, and access permittees; individuals who are DOE employees or applicants for DOE employment; and other persons designated by the Secretary of Energy for access to restricted data or special nuclear material, pursuant to the Atomic Energy Act of 1954, as amended, or for access to national security information (see <http://cfr.law.cornell.edu/cfr/>).
- g. DOE O 3731.1, *Suitability, Position Sensitivity Designations, and Related Personnel Matters*, dated 12-19-89, which identifies the interrelationships among suitability, security, and access authorizations; establishes guidance and policy regarding position sensitivity designations, certain background investigations, and suitability determinations; and establishes the policies and procedures regarding waivers of pre-employment investigations (see <http://www.directives.doe.gov/pdfs/doe/doetext/oldord/3731/o37311c1.pdf>).
- h. DOE O 142.1, *Classified Visits Involving Foreign Nationals*, dated 1-13-04, which establishes requirements and responsibilities for foreign national visits that involve access to classified information at DOE facilities (see <https://www.directives.doe.gov/pdfs/doe/doetext/restrict/neword/142/o1421.pdf>).
- i. DOE O 142.3, *Unclassified Foreign Visits and Assignments Program*, dated 6-18-04, which establishes requirements and responsibilities for foreign national visits that do not involve access to classified information at DOE facilities (see <https://www.directives.doe.gov/pdfs/doe/doetext/restrict/neword/142/o1423.pdf>).
- j. DOE M 470.4-5, *Personnel Security*, dated 8-26-05, which establishes objectives, requirements and responsibilities for the Personnel Security Program (see <https://www.directives.doe.gov/pdfs/doe/doetext/restrict/neword/470/m4704-5.pdf>).
- k. DOE M 470.4-2, *Physical Protection*, dated 8-26-05, which establishes requirements for physical protection of safeguards and security interests (see <https://www.directives.doe.gov/pdfs/doe/doetext/restrict/neword/470/m4704-2.pdf>).
- l. P.L. 93-579 (5 USC 552a), *Privacy Act of 1974*, which governs the collection and use of information by the Federal Government (see <http://www4.law.cornell.edu/uscode/>).
- m. P.L. 107-347 (44 USC 36), *E-Government Act of 2002*, which ensures sufficient protections for the privacy of personal information (see <http://www4.law.cornell.edu/uscode/>).

- n. OMB Memorandum M-03-22, *Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, which guides Agencies in conducting Privacy Impact Assessments in accordance with the E-Government Act of 2002.
 - o. DOE M 471.3-1, *Identifying and Protecting for Official Use Only Information*, dated 4-09-05, which establishes handling requirements for Official Use Only information (see <https://www.directives.doe.gov/pdfs/doe/doetext/restrict/neword/471/m4713-1.pdf>).
8. CONTACT. Questions concerning this Notice should be addressed to the Office of Chief Information Officer at 202-586-3768.

Formatted: Keep with next

Formatted: Bullets and Numbering

BY ORDER OF THE SECRETARY OF ENERGY:

CLAY SELL
Deputy Secretary

CONTRACTOR REQUIREMENTS DOCUMENT
DOE N 206.4, *PERSONAL IDENTITY VERIFICATION*

This Contractor Requirements Document (CRD) establishes the requirements for Department of Energy (DOE) contractors, including National Nuclear Security Administration (NNSA) contractors. Contractors must comply with the requirements listed in the CRD to the extent set forth in their contracts until such time as this CRD is superseded by a contract clause.

Regardless of who performs the work, contractors subject to this CRD are responsible for compliance with the requirements of the CRD and are also responsible for flowing down the requirements of the CRD to subcontracts at any tier to the extent necessary to ensure the contractors' compliance with the requirements.

1. **OBJECTIVE.** To apply the requirements of Homeland Security Presidential Directive 12 that certain individuals, to include DOE contractor employees, with access to DOE-owned or DOE-leased facilities be reliably identified and issued a security badge for such access. The contractor subject to this CRD will ensure that the identity proofing procedures discussed in this CRD are implemented into its procedures for investigation and issuance of DOE security badges.
2. **REQUIREMENTS.**
 - a. **Applicability.** The procedures described in this CRD apply to those management and operating contractors and other major facilities contractors authorized by DOE to process applications for a security badge, for personnel who require access to DOE-owned or DOE-leased facilities in the performance of their contracts.
 - b. **General.**
 - (1) DOE will only authorize issuance of security badges to individuals whose identities have been verified by a registrar in accordance with the identity proofing process discussed in this CRD. (DOE will not authorize the issuance of a security badge to any individual known or suspected by the Federal Government of being a terrorist.)
 - (2) Individuals who do not require a DOE security badge, including short term (6 consecutive months or less) uncleared contractors, but require access to DOE facilities are issued badges consistent with Departmental and local procedures. For short-term individuals, at a minimum, the following procedures will be implemented.
 - (a) Apply adequate controls to systems and facilities (i.e., ensuring short-term individuals have limited/controlled access to facilities).

- (b) Provide short-term individuals with clear documentation on the rules of behavior and consequences for failure to comply before granting access to facilities and/or systems.
 - (c) The badges issued to these short-term individuals must be visually distinguishable from security badges issued to individuals to whom Federal Information Processing Standards (FIPS) Publication (Pub) 201 does apply.
- c. Procedural Roles. Specific roles used in this process are defined under paragraph 3, “Definitions,” below.
- d. Procedures. As a precondition to DOE authorizing a security badge or otherwise granting access to a DOE facility to newly hired contractor employees with DOE access authorization (security clearance), and contractor employees without DOE access authorization (security clearance) designated by the applicable Departmental element, the contractor will ensure the following.
 - (1) The applicant is informed that the sponsor will make a request to the registrar on behalf of the applicant.
 - (2) The applicant provides the sponsor with his or her name, date of birth, position, and contact information for submission with the request to the registrar. When the contractor is the sponsor, the contractor will ensure that the sponsor’s name; organization; contact information, including the address of the contractor sponsor; and signature are provided to the registrar concurrent with each applicant’s initiating request.
 - (3) The applicant accurately completes and submits to the sponsor a Standard Form (SF) 85 or, for applicants who will require access authorization (personnel security clearance) an SF 86. When the contractor is the sponsor, the contractor will ensure that the contractor sponsor provides the applicant’s SF 85 or 86 to the registrar.
 - (4) The applicant appears in person before the registrar or registrar designee (Federal or contractor employee) with two original identity source documents. If the applicant is physically remote from the registrar, the registrar may designate an individual located in proximity to the applicant to act as registrar by proxy. The identity source documents must come from the list of acceptable documents included in Form I-9, OMB No. 1115-0136, *Employment Eligibility Verification*. At least one of the documents will be a valid State- or Federal Government-issued picture identification (see <http://www.uscis.gov/files/form/i-9.pdf>). The registrar will validate the applicant’s identity and original identity source documents and make a record copy for each identity source document. The registrar will also determine whether the applicant has a previous BI

Deleted: <http://uscis.gov/graphics/form/sfee/forms/files/i-9.pdf>

~~from either previous Federal employment or a previous position requiring an access authorization/personnel security clearance.~~

Deleted: The registrar will also check the applicant for previous BIs, either from

- (5) The applicant follows the registrar's direction for providing fingerprints and photograph for the BI request package, a copy of which will be retained by the registrar.
- (6) Once DOE authorizes the applicant's security badge, the applicant signs for and collects the security badge in person at the badge office (or at an office designated by the registrar to act as issuer) by presenting a valid State- or Federal Government-issued picture identity source document. (The issuer will validate the appearance of the applicant against the photograph on the identity source document and will validate the name and photograph of the security badge against those on the identity source document.)
- (7) The applicant acknowledges his/her understanding that if, subsequent to the issuance of the security badge, further processing of the BI by the registrar reveals derogatory information to be adjudicated under the criteria established in the DOE PIV Notice, DOE will determine the level of continued DOE badge and access privileges in accordance with current security procedures. Following this determination and based on the final resolution of the derogatory information badge and access privileges will either be revoked or reinstated as appropriate.

3. DEFINITIONS.

- a. Applicant. For the purposes of this CRD, an applicant is an individual applying for a DOE security badge through a DOE contractor or subcontractor.
- b. Registrar. The entity that establishes and vouches for the identity of an applicant to an issuer. The registrar authenticates the applicant's identity by verifying identity source documents and adjudicating a background investigation. The registrar ~~must be a Federal employee and will be appointed by the head of the appropriate Departmental/field element in writing.~~
- c. Registrar by Proxy. An additional federal employee appointed by the head of the Departmental/field element in writing to fulfill all registrar duties in a designated area.
- d. Registrar Designee. The registrar designee may be a federal or contractor employee assigned and designated by the registrar to perform only limited registrar functions, such as verifying I-9 documents, as designated by the registrar.
- e. Issuer. The organization that is issuing the security badge to an applicant. The badge may be issued by a Federal or contractor employee.

Deleted: or registrar proxy

Formatted: Bullets and Numbering

- f. Security Badge. A distinctive tag used for controlling access to facilities and security areas that provides an individual's name, photograph, and access authorization type and may include additional information in electromagnetic, optical, or other form.

- g. Sponsor. The individual who substantiates the need for a DOE security badge to be issued to the applicant and submits the request to the registrar. The sponsor may be a Federal employee or a DOE authorized major facilities contractor.

Deleted: management and operating

ACCREDITATION CHECKLIST FOR _____
 (Fill in Site)

Certification of Identity Proofing Process	Y/N
Implemented requirement to initiate a National Agency Check with Written Inquiries (NACI) or other suitability or national security investigation prior to DOE security badge issuance.	
Implemented requirement to receive the results of National Agency Checks prior to DOE security badge issuance [a DOE security badge can be issued based upon favorable results from the FBI National Criminal History Check (fingerprint check)].	
Implemented requirement to ensure that applicants appear in person at least once before a DOE security badge is issued.	
Implemented requirement to ensure that applicants provide two forms of identity source documents prior to DOE security badge issuance (the documents must come from the list of acceptable documents in <i>Form I-9, OMB No. 1115-0136, Employment Eligibility Verification</i> , and at least one must be a valid State- or Federal Government-issued picture ID).	
Implemented requirement to ensure that no single individual has the capability to issue a DOE security badge without the cooperation of another authorized person.	
Implemented requirement to ensure that no DOE security badge is issued unless requested by a proper authority.	
Implemented requirement for a revocation process that swiftly revokes expired or invalidated DOE security badges.	
Implemented requirement to ensure that personal information collected for employee and contractor identification purposes is handled in a manner consistent with the Privacy Act of 1974 (5 U.S.C. 552a).	
Implemented requirement to ensure DOE security badges are issued to DOE and contractor employees who require a DOE security badge.	
Implemented requirement to ensure people who do not require a DOE security badge but do require access to DOE facilities are issued badges consistent with Departmental policies and local practices.	
Implemented requirement to ensure that security badge issuance for Foreign National employee/contractors/visitors is done in accordance with DOE O 142.1, <i>Classified Visits Involving Foreign Nationals</i> , dated 1-13-04, and DOE 142.3, <i>Unclassified Foreign Visits and Assignments Program</i> , dated 6-18-04.	

References: FIPS 201, Section 2; OMB M 05-24, Implementation of HSPD 12

Check if Site does not issue DOE Security Badges

 Certifying Official Signature

 Date

 Certifying Official Printed Name and Title