Management System: Safeguards and Security		
Subject Area: Personnel Security		
Procedure: Implementing the Homeland Security Presidential Directive-12		
Issue Date: 08/23/2012	**Lead Subject Matter Expert:** Pat Vent or Shaun Meadows	**Management System Owner:** John Sattler

1.0 Applicability

This procedure applies to all EMCBC Federal and contractor employees who require a Homeland Security Presidential Directive (HSPD)-12 credential for physical and/or logical access to DOE facilities.

2.0 Required Procedure

Step 1	The Personnel Security Specialist checks the applicant's name in the Office of Personnel Management (OPM)'s database and/or the USAccess System to determine if the applicant has had a prior background investigation that will satisfy the investigation requirements for eligibility to an HSPD-12 credential.
Step 2	If no favorably adjudicated previous National Agency Check with Inquiries (NACI) or more complex type of background investigation has been conducted on the applicant, the Personnel Security Specialist enrolls the applicant in OPM's e-QIP system, or in the case of an applicant who requires a DOE security clearance, submits a SR-253, Clearance Request, to the Cognizant Personnel Security Office (CPSO).
Step 3	The applicant is sponsored for an HSPD-12 credential in the USAccess System.
Step 4	The applicant enrolls for the credential at a Credentialing Center.
Step 5	After the applicant completes the form in e-QIP, the appropriate investigation is initiated.
Step 6	Upon receipt from OPM, the investigative report is reviewed and adjudicated. The results of the adjudication are annotated in the USAccess system.
Step 7	The printed credential is issued to the applicant, who activates the credential at a Credentialing Center or at a Lite Activation Station.
Step 8	The certificates contained on the credential may not exceed the badge's expiration date, and will expire 3 years after they are initially activated. The certificates must be updated prior to their 3 year expiration in order to maintain

	the validity of the credential.
Step 9	A Personal Identification Verification (PIV) file is created for the applicant. The file holds a copy of the "Read and Understand" form which the applicant is required to sign upon receipt of his/her credential. This form identifies the applicant's responsibilities with respect to the credential.

3.0 References

- DOE O 473.3, Protection Program Operations
- Homeland Security Presidential Directive (HSPD)-12

4. Records Generated

The records table identifies those records generated during the work process described in any controlled document/procedure that shall be maintained to document activities or preserve historically valuable information after the work process is completed.

In accordance with IP-414-04, Quality Assurance Procedure, a determination needs to be made if these records are to be classified as quality assurance records. If it is deemed that these are quality assurance records, further classification of "lifetime" or "non-permanent" shall be made.

Records generated through implementation of this procedure are identified as follows, and are maintained by the (originating office or individual) in accordance with the EMCBC Organizational File Plan:

Records Category Code	**Records Title**	**Responsible Organization**	**QA Classification** **(Lifetime, Non-Permanent or N/A)**
ADM-18-22-A	Security Clearance/Access Authorization Case Records PIV (Personal Identification Verification Files)	Office of Technical Support & Asset Management	NA