

Pension Benefit  
Guaranty Corporation



# Order

**Subject: PBGC HSPD-12 Credential Issuance  
for Federal Employees and Contractors**

**Directive Number: GA 10- 11**

**Effective Date: 7/29/11**

**Originator: FASD**

**Alice Maroni  
Chief Management Officer**

- 
1. **PURPOSE.** This Order provides detail and direction in support of the PBGC implementation of the physical access requirements outlined in Homeland Security Presidential Directive-12 (HSPD-12) and further detailed in FIPS 201-1. It supports the requirement that all federal employees and contractors are suitably and reliably identified at all times. It also supports the requirement that the identification is based on sound criteria used to verify an individual's identity.

The HSPD-12 Directive defines secure identification as being:

- (a) Issued based on sound criteria for verifying an individual employee's identity
- (b) Resistant to fraud, tampering, counterfeiting and terrorist exploitation
- (c) Rapidly authenticated electronically
- (d) Issued only by providers whose reliability has been established by an official accreditation process.

This Order will be supplemented, where necessary, with more detailed PBGC information from the Entrance on Duty, Security Processing and Separation Clearance guidance provided by FASD.

2. **SPECIAL INSTRUCTIONS.** This Order implements Homeland Security Presidential Directive -12 (HSPD-12) at PBGC. Additionally, this Order covers the Physical Access Security components of HSPD-12 only. To date, Logical Access Security components have not been addressed.

Policies, processes and instructions previously developed to support the PBGC Facilities and Services Department (FASD) Personnel and Physical Security Program remain in effect to the degree that they support and supplement this Order. Revisions to this Order must comply with HSPD-12 and will take precedence over any other PBGC document that provides information related to the provision of federal credentials.

This instruction does not supersede PBGC Order PM 05-1, *Entrance on Duty and Separation Procedures*.

3. **SCOPE.** The provisions of this Order apply to all PBGC federal employees and contractors, and to any other personnel requiring access to PBGC offices.

4. **AUTHORITIES.** Statutes, regulations, executive orders and other authorities that govern PBGC programs and functions.

- a. Homeland Security Presidential Directive 12 (HSPD-12), *Policy for a Common Identification Standard for Federal Employees and Contractors*
- b. *Federal Identity Management Handbook*, U.S. General Services Administration, July 2005
- c. *Federal Records Act of 1950, as amended* (44 U.S.C. Chapters 21, 29, 31, 33, 35)
- d. NIST Federal Information Processing Standard 201-1, Change 1, *Personal Identity Verification for Federal Employees and Contractors*, March 2006
- e. NIST SP 800-73-2, *Interfaces for Personal Identity Verification*, September 2008
- f. NIST SP 800-76-1, *Biometric Data Specification for Personal Identity Verification*, January 2007
- g. NIST SP 800-79-1, *Guidelines for the Accreditation of Personal Identity Verification Card Issuers*, June 2008
- h. NIST SP 800-104, *A Scheme for PIV Visual Card Topography*, June 2007
- i. NIST SP 800-116, *A recommendation for the use of PIV Credentials in Physical Access Control Systems (PACS)*, November 2008
- j. OMB Circular A-130 Revised, *Management of Federal Information Resources*, 2000
- k. OMB Memorandum M-03-22, *Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*
- l. OMB Memorandum M-07-06, *Validating and Monitoring Agency Issuance of Personal Identity Verification Credentials*, January 2007
- m. PBGC Directive IM 15-1, *PBGC Records Management Program*, March 2009

- n. PBGC Directive PM-05-1, *Entrance on Duty and Separation Clearance Procedures for Federal Employees and Contractors*
- o. PBGC Directive PM 05-6, *PBGC Personnel Security and Suitability Program*, July 2006
- p. *Privacy Act of 1974, as amended* (5 USC § 552a).

5. **BACKGROUND.** HSPD-12 establishes the general requirements for a common federal identification system. The HSPD-12 directive mandates that all federal departments provide a process for the identity proofing and credentialing of federal employees and contractors to increase security and to provide greater interoperability between departments and federal facilities.

Based on Directive HSPD-12, NIST developed FIPS 201-1 “*Personal Identity Verification (PIV) of Federal Employees and Contractors*” which includes a description of the minimum requirements for physical and logical access to federal agency premises and systems. FIPS 201-1 consists of two parts, PIV (I) which satisfies the control objectives and meets the security requirements of HSPD-12, and PIV (II) which outlines the technical interoperability requirements of HSPD-12.

This Order applies the standards required to implement the PIV ( I) or physical security objectives of the HSPD-12 mandate.

6. **POLICY.** The Pension Benefit Guaranty Corporation (PBGC) requires that all federal employees and contractors who need repeated access to PBGC facilities and information systems are issued secure and reliable federal credentials. The federal credentials are based on the standards outlined in the National Institute of Standards and Technology (NIST) Federal Information Processing Standard (FIPS) 201-1, *Personal Identity Verification for Federal Employees and Contractors*. This Order describes PBGC’s responsibilities for implementing the NIST physical and personnel security standards for federal employees and contractors.

7. **DEFINITIONS.**

- a. **Activator.\*** The Activator issues the HSPD-12 credential to the Applicant following the completion of identity validation and background checks.
- b. **Adjudicator.\*** The Adjudicator is the federal employee delegated the duty to review and adjudicate all federal employee and contractor background investigations completed by the United States Office of Personnel Management (OPM).
- c. **Applicant.** The Applicant is the federal employee or contractor who requires scheduled and frequent access to a PBGC facility and needs to be credentialed to do so.

- d. **Designated Approving Authority (DAA).**\* The DAA is appointed by the Chief Management Officer (CMO) and approves all agreements associated with provisioning GSA Shared Services for HSPD-12.
- e. **Electronic Questionnaire Investigation Processing (eQIP) System.** The system which automates requests for personnel security investigations and clearances. All eQIP requests are submitted by a federal agency to OPM for the purpose of completing background investigations on the agency's federal employees and contractors. This is in compliance with the "e-Government Act of 2002."
- f. **eQIP Application.** An electronic application (i.e. the SF-85P, "Questionnaire for Public Trust Positions") used to collect required personal information in order to conduct a background investigation.
- g. **eQIP Welcome Letter.** Issued to each user of the eQIP system prior to their start date. The eQIP welcome letter grants the Applicant access to the eQIP system.
- h. **EOD.** Entrance on Duty, to be referred to as "EOD" in this document.
- i. **FASD.** Facilities and Services Department, to be referred to as "FASD" in this document.
- j. **Federal Manager.** Department Director, Division Manager, Supervisor or their designated alternate.
- k. **GSA.** United States General Services Administration, to be referred to as "GSA" in this document.
- l. **HRD.** Human Resources Department, to be referred to as "HRD" in this document.
- m. **HSPD-12.** Homeland Security Presidential Directive 12 is the directive that was issued for "Policy for a Common Identification Standard for Federal Employees and Contractors." HSPD-12 calls for all federal employees and contractors to use a standard "smart" credential to verify their identity for secure access to federal buildings and information systems. To be referred to as "HSPD-12" in this document.
- n. **Issuing Organization Security Officer (IOSO).**\* The IOSO is responsible for the suspension and/or revocation of PIV credentials.
- o. **Issuer.**\* Federal employee who inputs the applicant information into the USAccess system and produces and issues the PIV Credential. The Issuer has the power to revoke the PIV Credential due to an unsatisfactory background investigation.
- p. **Managed Services Office (MSO).**\* The GSA MSO is the executive agent responsible for managing government-wide acquisition of information technology to implement HSPD-12 services. The GSA MSO provides federal agencies with interoperable identity management and credentialing solutions that support HSPD-12 processes.
- q. **OIT.** Office of Information Technology, to be referred to as "OIT" in this document.
- r. **Personally Identifiable Information (PII).** Personal information (i.e., social security number, date of birth, or personal address), that can be used to identify an individual.

- s. **Personal Identity Verification (PIV).**\* A higher level of identity verification requirement established in HSPD-12 and FIPS-201.
- t. **Personnel and Physical Security Team (PST).** The PBGC PST is responsible for the day-to-day administration of the agency's Personnel and Physical Security Program.
- u. **PIV Credential.**\* Personal Identity Verification credential that is used by federal employees and contractors as a standardized form of identification that is secure, reliable and interoperable among federal agencies.
- v. **PIV Credential Issuance (PCI) Facility Manager.**\* The PCI Facility Manager is responsible for the daily operations of the PCI facility and defines and implements all operating procedures for the functions assigned to the PBGC PCI facility. The PCI Facility Manager also provides guidance on the standards adopted by the department.
- w. **Position Designation.** The position designation is the risk level afforded to a position. The Position Designation drives the type of background investigation type requested for each Applicant. The Position Designation process is outlined in PBGC Directive PM 05-6, *PBGC Personnel Security and Suitability Program*.
- x. **Registrar.**\* Federal employee responsible for identity proofing the Applicant and ensuring successful completion of the background checks. The Registrar provides the final approval for the issuance of a PIV credential to the Applicant.
- y. **Risk Level.** Also referred to as the "Suitability Risk Level". The risk level is an assessment of a position to determine its potential for adverse impact to the integrity or efficiency of the service and its effect on the agency or the agency's mission.
- z. **Role Administrator.**\* The Role Administrator initiates the process by assigning the appropriate, mutually exclusive role to the designated PST member.
- aa. **Senior Authorizing Official (SAO).**\* The SAO is responsible for the agency's implementation of the PIV Credential Issuance (PCI) Operations. The PBGC SAO is also the HSPD-12 Program Sponsor.
- bb. **Sponsor.**\* A Sponsor is an official representative from PBGC who substantiates the need for a PBGC HSPD-12 credential or temporary identification badge and attests to the validity of the Applicant requiring a PBGC HSPD-12 credential. The Sponsor initiates the enrollment process in the USAccess system.
- cc. **Technical Point of Contact (TPOC).** Similar to a COTR in duties. TPOCs administer Purchase Orders, Delivery Orders and GSA Task Orders.
- dd. **USAccess System.** The USAccess system is owned and operated by the U.S. General Services Administration (GSA). This system enables U.S. federal government agencies to credential employees, contractors, and affiliates.

---

\*Roles derived from NIST Federal Information Processing Standard 201-1,

Change-1, *Personal Identity Verification for Federal Employees and Contractors*, March 2006.

## **HSPD-12 CREDENTIAL OPERATIONS AND ISSUANCE ROLES, RESPONSIBILITIES AND PROCEDURES.**

PBGC uses the term “HSPD-12 processes” to refer to the PIV processes and “HSPD-12 credentials” to refer to the PIV credentials.

### **a. HSPD-12 Program Official Roles and Responsibilities**

- (1) **Senior Authorizing Official (SAO).** The Director of the PBGC Facilities and Services Department (FASD) acts as the SAO. The PBGC SAO will:
  - (a) Provide financial oversight and control
  - (b) Develop policy
  - (c) Exercise authority over all the functions and activities performed by the PCI facility.
- (2) **Designated Approving Authority (DAA).** The Manager of the Facility Services Division (FSD) acts as the DAA. The PBGC DAA will:
  - (a) Approve Service Level Agreements (SLAs)
  - (b) Approve Interconnection Security Agreements (ISAs)
  - (c) Approve Memoranda of Understanding (MOUs) with GSA Shared Services for HSPD-12.
- (3) **PIV Credential Issuance (PCI) Facility Manager.** The PST Lead Support Services Specialist acts as the PCI Facility Manager. The PCI Facility Manager will:
  - (a) Ensure that all HSPD-12 processes adhere to the requirements of NIST FIPS 201-1
  - (b) Ensure PBGC compliance with GSA and PBGC policies and procedures
  - (c) Lead the PBGC PST in the implementation of HSPD-12 processes.
- (4) **Personnel Security Team (PST).** The PBGC Personnel Security Team (PST) is responsible for the day-to-day administration of the agency’s Personnel and Physical Security Program. The PST will:
  - (a) Implement and execute all PBGC HSPD-12 processes in accordance with the requirements of NIST FIPS 201-1
  - (b) Execute all PBGC HSPD-12 processes in compliance with GSA and PBGC policies and procedures

- (5) **Privacy Official (PO).** The PBGC Privacy Officer acts as the HSPD-12 PO. The PO is responsible for addressing internal privacy related questions and concerns impacting the PBGC HSPD-12 process and policy.

**b. HSPD-12 Processing Roles and Responsibilities**

- (1) **Applicant.** The Applicant is the federal employee or contractor who needs to be credentialed. The Applicant will:
- (a) Complete the required background investigation forms as directed by Federal Manager or COTR
  - (b) Report to the PST Security Office for HSPD-12 processing
  - (c) Present two forms of identification as listed on Form I-9 (Note: at least one of those forms of identification must be a valid state or government issued picture identification (ID))
  - (d) Be fingerprinted and photographed.
- (2) **Sponsor.** The HSPD-12 Sponsor is a member of the PST. The Sponsor will:
- (a) Begin the HSPD-12 process upon receipt of EOD forms
  - (b) Initiate the ‚Enrollment Process’ in the USAccess System.
- (3) **Adjudicator.** The Adjudicator is a member of the PST. The Adjudicator will:
- (a) Review the results of the background investigation
  - (b) Determine suitability for Federal employment
  - (c) Record the adjudication decision in the USAccess system
  - (d) Inform the IOSO of the decision if the appeals process reveals unfavorable determinations.
- (4) **Issuing Organization Security Officer (IOSO).** The PST Lead Support Services Specialist acts as the IOSO. The IOSO will:
- (a) Investigate any potential identity anomalies, for example, suspected impersonation or mistaken identity
  - (b) View system logs and prepare reports on HSPD-12 program activity
  - (c) Revoke or reinstate an employee’s HSPD-12 credential after an investigation, based on advice from the Adjudicator



- (d) Remove or deactivate a credential holder or candidate in the USAccess system upon request from Human Resources (HR) or a member of the PST.

(5) **Activator.** The Activator is a member of the PST. The Activator will:

- (a) Meet with the Applicant in person
- (b) Verify the Applicant's identity before presenting them the card by:
  - i. Requesting and observing the Applicant's Government Issued ID, (one that was validated during the registration process)
  - ii. Validating the Applicant's fingerprint against the one embedded in the HSPD-12 credential
  - iii. Conducting a one-to-one fingerprint biometric check on the Applicant based on the requirements outlined in SP 800-76.
- (c) Secure the Applicant's signature attesting to the individual's acceptance of the HSPD-12 credential (The HSPD-12 credential will only be released after receiving the Applicant's signature)
- (d) Notify the Sponsor and Registrar that the HSPD-12 credential was issued/not issued to the Applicant
- (e) Maintain a record of the process after Activation is complete.

(6) **Registrar.** The Registrar is a member of the PST. The Registrar will:

- (a) Confirm the validity of the HSPD-12 request
- (b) Visually inspect and electronically validate the Applicant's identity documents
- (c) Copy and scan proof that the identity documents were presented and return them to the Applicant
- (d) Validate all the information by comparing Applicant information from different sources
- (e) Compile the information required for EOD and background checks into the Applicant's Security Case File
- (f) Photograph the Applicant (facial image)
- (g) Collect and record the Applicant's fingerprints
- (h) Complete the HSPD-12 Security Case File Checklist to track receipt of the applicant's personal information

- (i) Securely maintain and make available all information gathered throughout the HSPD-12 process so it is available for credential personalization.

(7) **Role Administrator.** The Role Administrator is the Manager of the Facility Services Division (FSD) and initiates the HSPD-12 enrollment process by assigning the Sponsor, Registrar, Adjudicator, and Activator roles to designated members of the PST.

## 8. HSPD-12 ENROLLMENT, ACTIVATION AND ISSUANCE PROCEDURES

### a. HSPD-12 Applicant Enrollment

#### (1) HSPD-12 Enrollment.

- (a) The Office of Human Resources or the Applicant's Contracting Officer Technical Representative (COTR) must submit the Applicant's personal information no later than 24 hours prior to EOD for the HSPD-12 Sponsor to initiate sponsorship (in the USAccess System).
- (b) The HSPD-12 Security Case File Checklist will be completed by the Registrar and used to track receipt of the applicant's personal information. The Registrar or a member of the PST and the applicant must co-sign the checklist to acknowledge receipt of the required documents.
- (c) Personal information received from each applicant will be stored in the applicant's HSPD-12 Security Case File. The Security Case File will remain within FASD and will be protected according to the requirements outlined for PII.
- (d) Photographs and Fingerprinting will be completed at the FASD Security Office located at PBGC headquarters.
- (e) The Applicant's photograph (head shot) must reflect his/her normal work appearance (e.g., if the applicant normally wears glasses then he or she should be wearing the glasses when photographed).

**(2) HSPD-12 Adjudication.**

- (a) OPM must receive the Applicant's background investigation forms within 14 days of EOD.
- (b) The Applicant's background investigation results must present no irregularities which preclude the applicant performing the assigned role based on the requirements defined in the PBGC Order PM 05-6, *PBGC Personnel Security and Suitability Program*.
- (c) PBGC's Interim ID Card and an Interim Security Access Card will be issued to the Applicant pending the completion of the background investigation.

**(3) HSPD-12 Approval.**

- (a) The HSPD-12 Adjudicator reviews the background investigation and makes an adjudicative decision; favorable or unfavorable.
- (b) Adjudicator enters all favorable or unfavorable actions into the "Adjudication" section of the USAccess system.
- (c) Favorable determination results in the release of applicant's information to GSA for card production and delivery.
- (d) Unfavorable determination results in the denial of an HSPD-12 credential.

**b. HSPD-12 Credential Issuance**

**(1) HSPD-12 Activation.**

- (a) The Adjudicator inputs favorable adjudicative results into the USAccess system. This step automatically releases the applicant's enrollment data to GSA for credential production.
- (b) The Activator receives the Applicant's credential and enters the credential into the USAccess Credential Card Inventory system. Upon completion of this step, the USAccess system automatically releases an email notification to the Applicant that their credential is ready for pick-up and instructs the Applicant to schedule their card pick-up and activation.
- (c) The Applicant appears in person by appointment in the FASD Security Office located in Suite 460.
- (d) The applicant completes the Activation process by providing a valid government-issued ID card (driver license, PBGC ID

badge or valid US passport) and provides finger print verification to validate identity.

- (e) The Activator will take the activated credential to the Issuer for programming physical access rights.

**(2) HSPD-12 Issuance.**

- (a) The Activator validates the Applicant's identity and the personal information on the credential against the identity source document produced by the Applicant at the time the credential is issued.
- (b) The Issuer activates the credential so that it grants the employee or contractor physical access to PBGC property.

**c. HSPD-12 Credential Use**

- (a) Employees and contractors use the HSPD-12 credential to gain access to PBGC facilities.
- (b) Employees and contractors are responsible for ensuring that the HSPD-12 credential is physically protected while in their care and for using the credential only within their scope of authority.
- (c) PBGC is responsible for managing the HSPD-12 credential applications and data to ensure that only the authorized user accesses its facilities and information using the credential.

**9. HSPD-12 CREDENTIAL RENEWAL, REISSUANCE AND REVOCATION PROCESSES**

This section outlines the processes surrounding HSPD-12 credential post-issuance activities.

**a. HSPD-12 Credential Management**

- (1) **HSPD-12 Credential Renewal.** An employee or contractor will be notified prior to the expiration of their credential by a member of the PST. In that event, the following steps are taken:
  - (a) The employee or contractor will be contacted by the PST at least 30 days prior to the expiration date (the date printed on the HSPD-12 credential) and they must complete the HSPD-12 credential renewal process prior by that expiration date.

- (b) The employee/contractor will be provided a link to the USAccess Scheduling Tool which they will use to schedule their enrollment appointment.
- (c) The Registrar will verify their identity, have a new picture taken and new fingerprints will be captured and verified.
- (d) The Adjudicator will request the reissuance of a new credential based upon renewal.
- (e) The PCI Facility Manager maintains a record of the credential renewal request for tracking purposes.

(2) **HSPD-12 Credential Reissuance.** An employee or contractor may request a new credential in the event of loss or damage of the original credential. In that event, the following steps are taken:

- (a) Employees or contractors shall report lost or stolen credentials to the PST, FASD immediately upon discovering that the credential is missing.
- (b) Upon receiving notice of a lost or stolen credential, the PST will suspend the credential, charge a replacement fee and initiate the credential reissuance process.
- (c) PBGC covers ½ the replacement cost of the credential of the first loss. Subsequent losses are paid in full by the employee or contractor to whom the credential was issued.
- (d) The PST will perform the entire identity proofing and enrollment process including image and biometrics capture prior to authorizing a replacement credential.
- (e) The PST issues a replacement credential.
- (f) The PCI Facility Manager maintains a record of the reissuance request for tracking purposes.

Note: Replacement cost is waived in situations where the loss is a result of theft or loss resulting in the filing of a police report or insurance claim.

**b. HSPD-12 Credential Denial and Revocation**

(1) **HSPD-12 Credential Denial.** At any time before the HSPD-12 credential is issued, information considered derogatory to a PBGC employee or contractor may be discovered. In that event, the following steps are taken:

- (a) The PST assesses the information to determine the impact to the employee's or contractor's suitability and initiates communications with the employee or contractor to validate

the information received and make a final suitability determination. In the event of an unfavorable determination:

- i. **Federal Employee.** The PST will contact HRD to implement the Adverse Action process described in PBGC Order, PM-05-6, *Personnel Security and Suitability Program*. A HSPD-12 credential will not be issued until a final action has been determined.
- ii. **Contractor.** Contractors will only be permitted to supply information to the PST to help mitigate a case prior to denial of the credential since they cannot access the services of the MSPB process.

(2) **HSPD-12 Credential Revocation.** At any time after the HSPD-12 credential is issued, information considered derogatory to a PBGC employee or contractor may be discovered. The removal of an employee or contractor due to an unfavorable suitability determination is a process defined in PBGC Order PM 05-6, *Personnel Security and Suitability Program*. The process below outlines the HSPD-12 Credential Revocation Process:

- (a) The PCI Manager assesses the information to determine the impact to the employee's or contractor's suitability.
- (b) If the information negatively affects the employee's or contractor's suitability, then the Suitability Process outlined in PBGC Order PM 05-6, *Personnel Security and Suitability Program* will be invoked to determine if action is warranted.
- (c) A suitability action resulting in an employee's or a contractor's removal from the agency will be communicated to the HSPD-12 Issuing Organization Security Officer (IOSO). The IOSO will authorize HSPD-12 credential revocation.

## 10. **HSPD-12 SECURITY, PRIVACY AND RECORDS MANAGEMENT RESPONSIBILITIES.**

### a. **PBGC HSPD-12 System Implementation and Security**

In response to HSPD-12 and in order to comply with the requirements outlined in the HSPD-12 program implementation, PBGC has executed an MOU with the GSA MSO. This MOU allows PBGC access to certified and accredited shared infrastructure and services which provide the following infrastructure elements:

- (1) Activation Stations
- (2) Centralized HSPD-12 Identity Management System

- (3) Card Production Facility
- (4) Card Activation, Finalization and Issuance service

PBGC Activation stations are located in the Facilities and Services Department, Suite 460, 1200 K St NW Washington DC. The activation stations are remotely linked to the GSA MSO via secure automated mechanisms. The PST is responsible for identity management, business management, program planning and communication with internal points of contact and with PBGC federal employees and contractors.

The GSA MSO is responsible for mitigating the risk of system compromise by taking appropriate technical and administrative security measures and by providing role based restrictions to system access. All data transmitted electronically from PBGC to GSA is encrypted en route. GSA maintains an audit trail of all system activity.

PBGC is responsible for ensuring that the physical security of the Activation Station is not compromised. All members of the PST are trained in their responsibilities to protect privacy data, and have undergone the appropriate background investigations. The USAccess System is designed with a report tool that can be utilized by those PST members holding a HSPD-12 role (Sponsor, Adjudicator, Security Officer, Role Administrator, Registrar/Activator) at any time. Additionally, more specialized reports can be requested from the GSA MSO which detail credential issuance and revocation activity and other HSPD-12 program statistics.

**b. Privacy**

The PBGC policy is to protect all information in a manner commensurate with their sensitivity and potential for misuse. All applicant information received by the PST, FASD, will be maintained consistent with the Privacy Act of 1974, as amended, the GSA USAccess Privacy Act Statement and PBGC's policy and procedures on the protection of PII.

**c. Disposition of Federal Records**

Electronic or paper files deemed official federal records will be saved as required by PBGC Order IM 15-1, *PBGC Records Management Program* and the Federal Records Act. Disposition of records will be performed in accordance with National Archives and Records Administration (NARA) and OPM records management regulations.

**11. REQUIRED FORMS.**

The table below lists all the forms required to comply with this Order and the time frames in which they must be submitted. All PBGC forms are available on the PBGC intranet. Requests for security processing forms can be emailed to the PST at [FASDSecurity@pbgc.gov](mailto:FASDSecurity@pbgc.gov).

<b>Forms required for PBGC HSPD-12 process</b>				
<b>Required Form</b>	<b>Due Date</b>	<b>HSPD-12 Activity Supported</b>	<b>Authorizing Official</b>	<b>Submit To</b>
PBGC Form 245, Staff Identification and Credential Request	DAY 1 EOD	Sponsorship	PBGC Manager or COTR/TPOC	FASD, Suite 460
PBGC Form 569, Building Security and Access Request	Up to 7 days prior to EOD	Sponsorship	PBGC Manager or COTR/TPOC	FASD, Suite 460
OF-306, Declaration for Federal Employment	No less than 24 hours prior to EOD	Background Investigation	N/A	FASD, Suite 460
eQIP Welcome Letter	No less than 24 hours prior to EOD	Background Investigation	N/A	FASD, Suite 460
I-9, Employment Eligibility Verification	DAY 1 EOD	Enrollment	HRD/FASD	Copy to FASD, Suite 460
Two forms of valid government-issued ID (see List A, B, & C on I-9)	DAY 1 EOD	Enrollment	HRD /FASD	FASD, Suite 460