Department of the Treasury

BUREAU OF ENGRAVING AND PRINTING

Personnel Security System (PerSec)

March 10, 2017

A. Contact Information

System/Project Name	**Personnel Security System (PerSec)**
OMB Unique Identifier	N/A
FISMA Number	N/A

1. Who is the person completing this document?	
Name / Title	**Derrik Oates; Security Engineer**
Office/Division	**OCIITS/ITAC**
Phone Number	**202-874-1692**
Email Address	**Derrik.Oates@bep.gov**

2. Who is the system owner?		
DCF Name/Title	**Stephen Hutchens, Deputy Chief**	**Thomas Klug, Manager**
Office/Division	**DCF Office of Security (OS)**	**WCF Security Division (SD)**
Phone Number	**(202) 874-2937**	**(817) 847-3927**
Email Address	**Stephen.Hutchens@bep.gov**	**Thomas.Klug@bep.gov**

3. Who is the system manager for this system or application?		
Name / Title	**Tamalyn Smith, Manager**	**Monique Bridges, Manager**
Office/Division	**DCF OS/Personnel Sec Branch**	**WCF SD/Personnel Sec Branch**
Phone Number	**(202) 874-1721**	**(817) 847-1911**
Email Address	**Tamalyn.Smith@bep.gov**	**Monique.Bridges@bep.gov**

Who is the Information System Security Manager who reviewed this document?	
Name / Title	**Michael Pease; Chief**
Office/Division	**Office of Critical Infrastructure and IT Security (OCIITS)**
Phone Number	**(202) 874-2651**
Email Address	**Michael.Pease@bep.gov**

Who is the Office/Bureau Privacy Officer who reviewed this document?	
Name / Title	**Anthony Johnson; Government Information Specialist (Privacy Act)**
Office/Division	**Office of Critical Infrastructure and IT Security (OCIITS)**
Phone Number	**(202) 874-2258**
Email Address	**Anthony.Johnson@bep.gov**

Who is the IT Reviewing Official?	
Name / Title	**Jose Pena; Acting Manager**
Office/Division	**OCIITS\ITAC**
Phone Number	**(202) 874-3229**
Email Address	**Jose.Pena@bep.gov**

B. System Application/General Information

1. Does this system contain any PII? [ ] No [X] Yes

2. What is the purpose of the system/application?

The BEP Personnel Security System (PerSec) is an integrated web-based case management system that provides investigatory information of employees and former employees, contractors and former contractors, applicants, and other individuals that have a recurring need to conduct business with BEP, such as Banknote Equipment Manufacturers (BEM) and Currency Reader Manufacturers (CRM). The Office of Security, Personnel Security Division (PSD-DCF) and the Security Division, Personnel Security Branch (PSB-WCF) will replace the current Employee Suitability System (ESS) Microsoft Access Database with PerSec.

PSD and PSB assign a Personnel Security File (PSF) to each individual under investigation. The PSF is used to determine:

1. Eligibility for physical and/or logical access to BEP facilities or its IT network;
2. Eligibility to hold sensitive positions including but not limited to eligibility for access to classified information;
3. Suitability or fitness for Government employment and/or qualification to perform work on behalf or for the U.S. Government as a contractor;

Investigatory information provided by PerSec is part of the individual PSF. PerSec will allow PSB and PSD personnel (i.e. Security Analysts, Investigators, and Adjudicators) to:

- Track monthly and annual financial and criminal history checks for national security and eligible positions included in the Federal Government's Continuous Evaluation Program (CEP).
- Track cases assigned to PSB and PSD staff responsible for conducting, adjudicating, and managing background investigations, internal investigations, employment suitability determinations, and security clearances.
- Tracks cases and security clearances throughout their lifecycle.
- Record investigative requests made to the Office of Personnel Management (OPM) and billing receipts of those requests.
- Automate manual/paper business processes, such as performance tracking, approval workflows, and internal form generation/management.
- Record internal Security/Special Investigations (SI) on employees and contractors in response to suspected or actual misconduct or criminal behavior incidents.
- Use a comprehensive reports management module.

- Retrieve personnel information, including Standard Form-86 (SF86), e-QIP information, and manually ingest and store information associated with the individual.

- Compile national security clearance data into a flat file (single table of data) for clearance validation. This file is the required file format for uploading validation data to OPM's Central Verification System (CVS). Agencies are required to validate National Security Clearance data every month in CVS to maintain required reciprocity of investigations and clearances government-wide. Generate the following investigatory records about an individual and store them with the applicable case in PDF format:

    - Report of Investigation (ROI);
    - Local Agency Check (LAC) Request Letters;
    - Adjudication Summary Report (ASR);
    - BEP Form 2357 - Notification of Personnel Security/Suitability Determination; and
    - Department of the Treasury Directive TD F 15-03.2 - Department of the Treasury Certificate of Clearance and/or Security Determination.

The PSB and PSD are responsible for conducting monthly updates to ensure data validity and accuracy. BEP will update the associated Privacy and Civil Liberties Impact Assessment (PCLIA) prior to using new PII or employing new internal or external interfaces.

3. What legal authority authorizes the purchase or development of this system/application?

31 U.S.C. § 321, 44 U.S.C. § 3544, 5 C.F.R. § 731, 5 C.F.R. § 732, Executive Order 9397, 8 Fed. Reg. 16095 (November 30, 1943) as amended by Executive Order 13478, 73 Fed. Reg. 70239 (November 20, 2008), Executive Order 10450 as amended, 18 Fed. Reg. 2489 (April 27, 1953), Executive Order 12968 as amended, 60 Fed. Reg. 40245 (August 7, 1995), Executive Order 13467, 73 Fed. Reg. 38103 (July 2, 2008) and Homeland Security Presidential Directive 12 (HSPD-12).

4. Under which SORN does the system operate? (Provide name and number)

SORN coverage is provided by Treasury/BEP .021 Investigative Files, 73 Fed. Reg. 22604 (April 16, 2013) and Treasury .007 Personnel Security System, 81 Fed. Reg. 78266 (November 7, 2016).

C. Data in the System

1. **What categories of individuals are covered in the system? (e.g., employees, contractors, taxpayers, other)**

   The system covers BEP employees and former employees, contractors and former contractors, applicants, and other individuals that have a recurring need to conduct business with BEP, such as Banknote Equipment Manufacturers (BEM) and Currency Reader Manufacturers (CRM) that receive new designs and production samples of Federal Reserve notes (FRNs).

2. **What are the sources of information in the system?**

   a. **Is the source of the information from the individual or is it taken from another source? If not directly from the individual, then what other sources?**

      BEB obtains information directly from an individual's personal testimony and submitted documents. BEP receives additional information from federal, state, local, or tribal law enforcement agencies, credit bureaus, financial institutions, courts of law, educational institutions, individuals contacted as references, or sources developed by the investigator through contact at previous employers or residences.

   b. **What Federal agencies are providing data for use in the system?**

      BEP obtains information from various federal agencies but primarily from OPM and the Federal Bureau of Investigations (FBI). However, additional federal agencies such as the Internal Revenue Service (IRS), Department of Defense (DOD), Department of State, Department of Homeland Security (DHS) and its many immigration agencies also provide information. BEP may contact other federal agencies seeking additional background information to develop a "whole person" view prior completing the investigation. The PerSec-generated ROI contains this additional information in its synopsis and attached hard copy documents that will be placed in the individual's PSF.

   c. **What state and/or local agencies, tribal governments, foreign governments, or international organizations are providing data for use in the system?**

      BEP obtains data related to the individual from state, local, or tribal law enforcement agencies and/or courts of law with jurisdiction over localities where the individual lives or lived previously.

   d. **From what other third party sources will data be collected?**

      BEP may collect data during the background investigation process from third party sources such as credit bureaus, financial institutions, courts of law, educational institutions, individuals contacted as references, or sources developed by the investigator through contact at previous employers or residences. BEP may

also receive information from organizations or associations which the individual may be a member.

e. What information will be collected from employees, government contractors and consultants, and the public?

PerSec records contain the following PII and information related to the specific coverage period for the current investigation:

- Full Name;
- Other names used;
- Date of birth;
- Place of birth;
- Social Security number (SSN);
- Height;
- Weight;
- Hair Color;
- Eye Color
- Gender;
- Marital Status;
- Full name, maiden name and other names used, date of birth, contact information, and citizenship of current or former spouses and dates of marriage;
- Cohabitant full name and other names used, date of birth, contact information, and citizenship of current or former spouses and date cohabitation began;
- Current and former home addresses (including dates of residence);
- Home, work, and mobile phone number;
- Citizenship Country;
- U.S. Passport Information (including passport number, issue date, expiration date, and name in which passport was first issued);
- Countries traveled to while on current passport and dates involved with each;
- Name, address, and contact information of neighbor or other known associates;
- Schools attended (including locations, dates attended, name of person who knew you at the school and their contact information, if available);
- Degree/Diploma attained and dates awarded;
- Employment Type;
- Employment history (including name and contact information of supervisor, if available);
- Military service history (including type of discharge);
- Selective Service Registration information;
- Type of relatives;

- Full name of relatives (including date of birth, place of birth, country of citizenship, and name of employer (if not a U.S. citizen but has a U.S. address).
- Name of foreign contacts (including dates of first/last contact, contact information, date of birth, place of birth, and country of citizenship, if available;
- Foreign activities (including stocks, property, investments, bank accounts, ownership of corporate entities, corporate interests or business);
- Foreign travel (including country and dates visited);
- Psychological and emotional health history;
- Police record information;
- Credit reporting information;
- Information obtained from IRS pertaining to income tax returns;
- Involvement in Non-Criminal Court Actions;
- Illegal use of drugs and drug activity;
- Alcohol use information;
- Investigations and clearance record (including level of clearance, name of investigating agency, agency issued the clearance eligibility/access; date investigation completed, and date clearance/access granted;
- Investigation results and/or summaries;
- Investigation supporting information provided by the investigating agent or other agencies;
- Financial Record;
- Use of Information Technology Systems information; and
- Association Record (including name and contact information of organization).

PerSec will generate the following forms and/or documents and store them with the applicable case in PDF format. The PerSec PCLIA will state the data elements associated with these forms and/or documents:

- Report of Investigation (ROI), which contains:
  - Name;
  - Case Number, Case Type, Appointment, Position Risk, and Position Sensitivity;
  - Date of Birth;
  - Place of Birth;
  - Work Location, Position, Grade, and Division/Branch
  - National Security Clearance Level, and date granted;
  - Date case opened;
  - Results of information obtained from the SF-86 and investigator remarks;
  - Results of the National Agency Check (NAC);
  - Results of the Credit Check;
  - Signature of Investigator and date signed; and

- Signature of Adjudicator and date signed.

- Local Agency Check (LAC) Request Letters, which contain:
  - Investigation Subject's Name, Maiden Name (if applicable), and other names uses;
  - Social Security number (SSN)
  - Date of Birth;
  - Place of Birth; and
  - Gender.

- Adjudication Summary Report (ASR);
  - Investigation Subject's Name;
  - Case Number;
  - Summary of Investigative Results;
  - Concerns/Adjudication Summary Determination;
  - National Security Clearance/Eligibility Determination;
  - Report of Agency Adjudication to OPM;
  - Administrative Actions taken and date; and
  - Any attached documents (e.g. ROI, NAC).

- BEP 2357 - Notification of Personnel Security / Suitability Determination, which contain:
  - Investigation Subject's Name;
  - Social Security number (SSN);
  - Date of Birth;
  - Position Title, Contract Company Name, or other Government Agency Name;
  - Type of Request;
  - Case Type;
  - Risk Level;
  - Sensitivity;
  - Final Determination; and
  - Signature of Adjudicator and date signed.

- TD F 15-03.2 - Department of the Treasury Certificate of Clearance and/or Security Determination.
  - Bureau Name;
  - Investigation Subject Name;
  - Social Security number (SSN);
  - Grade;
  - Date of Birth;
  - Place of Birth;
  - Position Title and Official Assignment;
  - Date Investigation Completed;
  - Type of Investigation Conducted;
  - Agency Which Conducted Investigation;

- Highest Classification of Information Authorized to Access;
- Date Interim & Final Clearances Granted;
- Any Remarks; and
- Name, Title, Signature of Security Official, and date of signature.

Fingerprints or fingerprint activities are not part of the PerSec at this time. They are handled separately.

3. Accuracy, Timeliness, and Reliability

a. How is data collected from sources other than from Treasury records going to be verified for accuracy?

PSB and PSD users create a profile in OPM's electronic Questionnaire for Investigative Processing (e-QIP) for each person under investigation and assign the appropriate investigative form for the individual to complete. If the form lacks information, it is rejected back to the individual for correction and re-certification. The individual certifies that their information is correct and true to the best of their knowledge prior to release of the electronic security forms to PSB and PSD. No electronic interface exists at this time between e-QIP and PerSec. Any data obtained from e-QIP will be manually transferred to PerSec. The PSB and PSD Investigator assigned the case will review the data with the individual during a Subject Interview and verify its accuracy. If there is incorrect information or the Investigator requires and explanation, the Investigator will annotate the discrepancies in the ROI and request that the individual provide a Voluntary Statement, in writing, that explains or clarifies the information.

Information obtained as records from federal, state, local, or tribal government agencies or courts of law pursuant to federal or state laws and regulations regarding records verification and retention are presumed accurate. Information obtained from neighbors, co-workers, friends, supervisors, and when necessary, family members, is presumed accurate when two or more individuals corroborate the obtained information.

Data within PerSec may be reviewed by the Personnel Security National Security Point of Contact (NSC POC) when another government agency requires verification of a BEP employees' national security clearance or eligibility for a clearance, in order for the BEP employee to gain access to that agency's facilities or its sensitive information. The Personnel Security NSC POC may contact another agency NSC POC to request that agencies background investigation or to verify clearance of one of their employees for temporary access to the BEP.

b. Is completeness required? [ ] No [X] Yes

c. What steps or procedures are taken to ensure the data is current and not out-of-date?

The individual's PII is taken directly from the data collected in e-QIP and used to open an initial case record in PerSec. Once the PII is in PerSec, all subsequent investigations require only the individual's SSN to open a new case record. For subsequent records, PerSec automatically populates all PII fields. The PII in PerSec is confirmed accurate and up to date by comparing the PII and position title in PerSec with the PII and position title with the Human Resource Employment Verification Report. The Office of Human Resources provides this report to PSB and PSD on a monthly basis and it is used to complete a full audit of the PII on subjects of the investigation in PerSec each year.

During current investigations, PSB and PSD personnel (i.e. Security Analysts, Investigators, and Adjudicators) update numerous data fields as the investigation progresses or upon receipt of additional information. All positions designated Moderate, High Risk, and Non-Critical or Critical Sensitive must undergo a periodic reinvestigation every five (5) years. BEP verifies that all associated information is current and accurate. There are no requirements to re-investigate individuals that have a Low Risk designation. However, BEP Office of Security verifies and validates all badge holders on an annual basis.

d. Are the data elements described in detail and documented? [x] No [ ] Yes If yes, what is the name of the document?

Although PerSec will store PII listed within the SF-86 and other security forms and documents, the automated data fields will not mirror the SF-86 in this iteration. Once PerSec establishes an interface with the e-QIP and HRConnect Systems, it will mirror the elements listed in Section 3 above. BEP will list those data elements in the PerSec System Design Document (SDD) prior to the next phase.

D. Attributes of the Data

1. Is the use of the data both relevant and necessary to the purpose for which the system is being designed? [ ] No [X] Yes

The information gathered and compiled into the ROI, is relevant, necessary and essential to the purpose of its design.

2. Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected, and how will this be maintained and filed? [] No[X] Yes

By its very nature, a background investigation assimilates information that does not originate from a single location, such as medical, financial, criminal or employment records, or from third parties collected through interviews. Although the system collects new data, it does not use the data in such a manner that would constitute datamining by

developing predictive patterns or trends associated with the individual. The information is maintained both electronically in PerSec and manually in the PSF.

3. Will the new data be placed in the individual's record? [ ] No [X] Yes

The PerSec case record will contain all data obtained related to an individual and will be placed in their PSF.

4. Can the system make determinations about employees/members of the public that would not be possible without the new data?

No. As the data collection mechanism for the investigation, the PerSec system does not directly make determinations about an individual. However, the investigative information obtained and stored in PerSec will allow PSB and PSD personnel to make employment suitability determinations about individuals.

5. How will the new data be verified for relevance and accuracy?

See response to 3a, 3b and 3c above.

6. If the data is being consolidated, what controls are in place to protect the data from unauthorized access or use?

PerSec resides on a secured network within the FedRamp Certified Government Cloud Services framework. Access to PerSec is limited to PSB and PSD personnel (i.e. Security Analysts, Investigators, and Adjudicators) and selected personnel within the Office of Human Resources (OHR). These users will have limited access to the system on a need-to-know basis. Role-based access controls are employed to limit the access of information by different users and administrators based on the need-to-know the information for the performance of their official duties.

The PerSec IT Specialist and IT Contractors manage the system for IT security purposes. Once IT provides a user access to the PerSec security pool on the network, the Personnel Security System Administrators creates a User Profile in PerSec and grants levels of access within PerSec. Each case record is assigned an access level of 1, 2 or 3. Level 1 records are generally those associated with senior management personnel at the GS14 level and above. Level 2 records are generally first line supervisory positions. Level 3 constitutes the general user population of employees in PSB and PSD or other authorized users.

The PSF records are maintained in locked file cabinets or GSA approved safes. Both the PSF's and PerSec network sites are located in rooms that are accessed only by card reader. Only authorized personnel have access to the rooms and authorized users (with PerSec profiles) have access to the PerSec data.

7. If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? Explain.

Processes are not being consolidated. However, there are numerous controls in place to protect the data and prevent unauthorized access. PerSec inherits a majority of its security controls from the BEP Local Area Network (LAN) and Wide-Area Network (WAN). PerSec access controls are multi-layered with IT Security limiting access to the application by establishing membership in an Active Directory security group for access to the system. Personnel Security System Administrators create internal system profiles and assigns the roles within the system. This prevents unauthorized access to PerSec.

8. How will the data be retrieved? Is the data retrieved by a personal identifier? If yes, explain and list the identifiers that will be used to retrieve information on the individual.

PerSec will retrieve information by SSN, name of the individual, case number and/or age of the case.

9. What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?

Each individual has a Personnel Security File (PSF) and an Adjudicative Summary Report (ASR) containing all investigatory information that is used to determine:

1. Eligibility for physical and/or logical access to BEP facilities or its IT network;

2. Eligibility to hold sensitive positions including but not limited to eligibility for access to classified information;
3. Suitability or fitness for Government employment and/or qualified to perform work on behalf or for the U.S. Government as a contractor;

Investigatory information provided by PerSec is part of the individual's PSF.

PerSec records are assigned unique case numbers to identify the electronic investigative record within PerSec. PerSec formats the collected data into a Report of Investigation (ROI) and the Adjudicative Summary Report (ASR).

The information gathered is required to define a "whole person" concept that allows the PSB and PSD personnel to make informed suitability and/or security-related decisions. The system also provides the ability to track the risk/sensitivity level of investigations conducted and provides reports displaying individuals that (1) have been granted national security clearances, (2) are eligible for a clearance but don't currently hold an active clearance, and (3) identifies individuals that require a five year periodic reinvestigation.

PerSec does not generate any of OPM's investigative forms such as: SF-85, SF-85P or the SF- 86.

PerSec will generate the following records and store them with the applicable case in PDF format:

- Report of Investigation (ROI);
- Local Agency Check (LAC) Request Letters;
- Adjudication Summary Report (ASR);
- BEP Form 2357 - Notification of Personnel Security/Suitability Determination; and
- Department of the Treasury Directive TD F 15-03.2 - Department of the Treasury Certificate of Clearance and/or Security Determination.

Access to this information is generally restricted to PSB and PSD personnel staff initiating or conducting the investigation or making the suitability/security determination(s).

E. Maintenance and Administrative Controls

1. If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?

The PerSec system resides on the BEP network at DCF. The WCF will access the system through a remote desktop connection. This process ensures usage and data consistency.

2. What are the retention periods of data in the system?

All investigative records are maintained for the duration of an individuals' employment or need for access. Records are retained in accordance with the National Archives and Records Administration (NARA) General Records Schedule (GRS) No. 18 (NC1-GRS-80-1, items 21, 22, 23, and 24. The following retention periods apply:

- Security Clearance Administrative Subject Files are destroyed when 2 years old. (NC1-GRS-80-1 item 22).

- Personnel Security Clearance Files are destroyed upon notification of death or not later than 5 years after separation or transfer of employee or no later than 5 years after contract relationship expires, whichever is applicable. (NC1-GRS-80-1 item 23a).

- Personnel Security Clearance Status Files are destroyed when superseded or obsolete. (NC1-GRS-80-1 item 24).

- Security Violations Files are destroyed 5 years after close of case. (NC1-GRS-81-8 item 1a) and all other files, exclusive of documents placed in official personnel folders are destroyed 2 years after completion of final action. (N1-GRS-98-2 item 31).

3. What are the procedures for disposition of the data at the end of the retention period? How long will the reports produced be kept? Where are the procedures documented?

The PSF ROI paper case records that reach the end of their retention period are destroyed by shredding or burning. Electronic records pertaining to former employees and contractors are made inactive prior to transferring them to an archive until they reach the end of their approved retention cycle. Electronic investigative records that reach the end of their retention period are electronically erased from the Archive Menu using accepted and approved techniques. This manual function is normally performed by the Personnel Security System Administrator.

Reports generated that are not a part of the investigative files are retained in accordance with NARA GRS No. 18 (NC1-GRS-80-1 item 21).

The procedures used to facilitate this process are documented in BEP Circular No. 80-05, Records Management Program (2006); BEP Circular No. 80-05.3, Records Storage (2007); and BEP Circular No. 80-05.4, Policies and Procedures for Electronic Records and Email (2006).

4. **Is the system using technology in ways the office or bureau has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)? If yes, explain.**

   No. The system does not use any previously unemployed technologies.

5. **How does the use of this technology affect public/employee privacy?**

   The technology enhances privacy by providing an infrastructure to manage PII-related activities that were previously managed manually in paper form. PerSec automates these manual processes and procedures and stores the information in a secured data network.

6. **Will the system provide the capability to identify, locate, and monitor individuals? If yes, explain.**

   Yes. Although PerSec and the background investigation/national security process allows users to identify a user and locate the users business location and residences, it does not provide the means to monitor an individual's movements or monitor their activities in real-time. PerSec is merely a tool to facilitate document handling and case management for employment suitability and/or access to national security information.

7. **What kind of information is collected as a function of the monitoring of individuals?**

   Not applicable. No one is monitored via this system.

8. **What controls will be used to prevent unauthorized monitoring?**

   Not Applicable.

9. **Under which SORN does the system operate? (Provide name and number)**

Treasury/BEP .021 Investigative Files, 73 Fed. Reg. 22604 (April 16, 2013)
Treasury .007 Personnel Security System,
81 Fed. Reg. 78266 (November 7, 2016).

10. If the system is being modified, will the SORN require amendment or revision? Explain.

PerSec is a new system that and is not being modified. This PIA is being generated to support the initial Security Assessment and Authorization (SA&A). The associated SORNs will be reviewed and updated once PerSec alters the PII contained in the system when BEP establishes an electronic interface with e-QIP and HRConnect.

F. Access to Data

1. Who will have access to the data in the system? (e.g., contractors, users, managers, system administrators, developers, others).

Access to data in the system is limited to the PSB and PSD personnel, the IT Specialist, and approximately two, IT Contractors that manage the system. Each of these individuals have been granted membership in an Active Directory security group for access to the system and have user profiles and assigned roles in the system. Other BEP stakeholders including but not limited to the Office of Security's Drug Free Workforce Program, and the Office of Human Resources (OHR) will have limited access to the system on a need-to-know basis. Role-based access controls are employed to limit the access of information by different users and administrators based on the need-to-know the information for the performance of their official duties.

PerSec Managers at DCF and WCF determine which role a prospective user requires and the Personnel Security System Administrator then creates a User Profile in the system and assigns that Profile to a Group Role. There are instances where other BEP offices will request access to the data. This request will be reviewed and if approved, PerSec Administrators will direct IT Security to grant the individual membership into the Active Directory. At this point, the Personnel Security System Administrator will create a User Profile in the system and assign the PerSec Case Guest role limiting access to the data on a need-to-know basis.

2. How is access to the data by a user determined? Are criteria, procedures, controls, and responsibilities regarding access documented?

The standard BEP Identity and Access Management System procedures are used to request, review, and approve an individual's access to PerSec. The BEP Active Directory is used to enforce a user's data access rights based on the roles they have been assigned. The following are the Group Roles within the system the Personnel Security Administrator assigns:

User Class	Business Roles	Pertinent characteristics of User Class
Guest	HR specialist, Drug Free Workforce Program Personnel	Perform queries, Read-Only Function
Operations/ Security Analyst	Program Support Assistant, Program Support Analyst	Initiates cases, Perform queries, standard and ad-hoc reporting
Adjudicator	Adjudicator	Initiates cases, Perform queries, Standard and ad-hoc reporting, Modifies Cases
Investigator	Investigator	Initiates cases, Perform queries, Standard and ad-hoc reporting, Modifies Cases
Manager	Adjudicating Supervisor, Investigative Branch Manager	Workflow Approvals, Dashboard Monitoring, Standard and Ad-Hoc Reporting
System Administrator	System Administrator	Full System Access

3. **Will users have access to all data on the system or will the user's access be restricted? Explain.**

   See F.1 and F.2 above.

4. **What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those having access? List procedures and training materials.**

   The internal system roles determine the scope of functions and data that are exposed to a member of that role. The roles control or limit access to data based on proximity to the user. For example, a user may not see or process an investigation pertaining to them. Most roles preclude the user from seeing the cases of (1) employees within their organizational unit, (2) their manager/supervisors, (3) senior management officials unless they are assigned that particular investigation, and (4) investigations assigned to a different BEP facility. There are no system-based training modules at this time. All users of the system are required to take Annual Privacy Awareness and Security Awareness Training.

5. **Are contractors involved with the design and development of the system and will they be involved with the maintenance of the system?**

Contractors, in collaboration with BEP IT Security and DCF Office of Security-Personnel Security Division developed the PerSec system. Support and maintenance of the system is managed by BEP IT staff with system work assignments given to IT contractors and reviewed by BEP IT personnel. There is a Privacy Act clause included in the current maintenance contract.

6. Do other systems share data or have access to the data in the system? If yes, explain.

PerSec resides within BEP's FedRamp Certified Government Cloud Services framework (Salesforce). PerSec only shares data with the Active Directory at this time. In the future, BEP will interface with the e-QIP and Treasury HRConnect Systems. Although BEP anticipates using a web-based interface in the future to leverage personnel data contained in the Department of the Treasury HRConnect System and the Office of Personnel Management's (OPM) e-QIP System, it will not do so in this iteration.

7. Who will be responsible for protecting the privacy rights of the public and employees affected by the interface?

All personnel that have access to PerSec are responsible for protecting the privacy rights of employees and former employees, contractors and former contractors, and members of the public.

8. Will other agencies share data or have access to the data in this system?

[X] Federal [X] State [X] Local [X] Other

9. How will the data be used by the other agency?

PerSec information may be shared with OPM, the FBI, and other federal, state, local, or tribal law enforcement agencies to facilitate the background investigation, employment suitability, and national security program management processes. This information is also shared as necessary to facilitate National Security Clearance reciprocity, access to controlled facilities, and issuance of PIV cards in support of HSPD-12. The information will also be shared in accordance with the Privacy Act and the routine uses identified in the SORNs listed in Section 4 above.

10. What are the procedures that allow individuals to access their information?

Individuals seeking notification of and access to any record contained in these systems of records, or seeking to contest its contents, may submit a request in writing to the BEP Disclosure Officer, whose contact information and submission instructions can be found at https://www.moneyfactory.gov/foia.html.

11. Who is responsible for assuring proper use of the data?

All personnel with access to PerSec are responsible for assuring proper use of the data.

The Following Officials Have Approved This Document

1. **System Owner**

   Name: Tamalyn Smith (for Stephen Hutchens)

   (Signature) **Date**

   Name: Thomas L. Klug

   (Signature) **Date**

2. **System Manager**

   Name: Monique Bridges

   (Signature) **Date**

   Name: Tamalyn Smith

   (Signature) **Date**

3. **Information System Security Manager**

   Name: Michael Pease

   (Signature) **Date**

4. **Privacy Point of Contact**

   Name: Anthony Johnson

   (Signature) **Date**

5. **IT Review Official**

   Name: Jose Pena

   (Signature) **Date**

6. **Deputy Assistant Secretary for Privacy and Treasury Records (when necessary)**

   Name:

   (Signature) **Date**