Department of the Treasury
BUREAU OF ENGRAVING AND PRINTING

Integrated Security System (ISS)

November 22, 2016

A. System Application/General Information

1. **Does this system contain any Personally Identifiable Information (PII)? [ ] No [X] Yes**

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

   The Integrated Security System (ISS) is a multi-process Commercial-off-the-Shelf (COTS) physical access control system (PACS) customized and used by BEPs Office of Security to manage access to its facilities, including the District of Columbia Facility (DCF) and Western Currency Facility (WCF). ISS provides an open/flexible architecture for integrating various subsystems and security devices for monitoring and access control at BEP facilities.

   The purpose of the system is to maintain a record of those persons who enter BEP's property and the time and areas visited. Specifically, ISS:

   - Monitors, controls, and manages physical access control authorizations to BEP facilities, and security sensitive areas;
   - Captures alarm events, and the time and location of such events;
   - Verifies credential authenticity and authentication of individuals seeking access to secure areas;
   - Manages physical intrusion detection;
   - Generate reports; and
   - Monitors and controls Closed Circuit Camera (CCTV) technologies and components, which allows system personnel to manage cameras during normal operations and in response to alarm events.

   ISS performs the following functions and their associated systems:

   - WCF:
     1. Data Acquisition System (DAS);
     2. Video Badging Computer; and
     3. Original Integrated Security System (ISS).
   - DCF:
     1. Access Control Alarm Monitoring System (ACAMS); and
     2. Video Badge System (VBS).

BEP will migrate the existing data/records, including any PII, from existing systems to ISS either by export/import utilities or manually.

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

5 U.S.C. § 301; 31 U.S.C. § 321; 31 C.F.R. § 605.1

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

TREASURY/BEP .027 Access Control and Alarm Monitoring Systems (ACAMS), 78 Federal Register 22604 (April 16, 2013), which is available at: https://www.treasury.gov/privacy/issuances/Documents/2013-08849.pdf.

B. Data in the System

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

- Employees, contractors, service company employees, and other U.S. Government agency employees, who have been cleared for access to BEP and issued a BEP Security Access Control (SAC) badge; and

- Escorted visitors such as contractors and service company employees who have not undergone the formal clearance to enter the BEP and issued a Visitor badge (This program does not pertain to individuals taking BEP limited area public tours).

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?**

ISS receives its information directly from the individual, their supervisor, the Department of the Treasury's HR Connect portal, from individuals submitting information on behalf of a visitor from other agencies or commercial companies conducting business with BEP, and from the employee's assigned General Service Administration (GSA) Personal Identity Verification (PIV) badge.

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

The General Service Administration (GSA) and the Department of the Treasury, and BEP Departmental Offices provide data used in the system.

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

None.

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

None.

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

BEP will collect the following information from employees, contractors, commercial company employees, and members of the public who have requested and have been cleared for entry and issued a SAC or Visitor badge to access BEP property:

- Photograph;
- Full name;
- Name of Company (for non-BEP personnel);
- Supervisory status;
- Section (specific area in the building);
- Date access badge issued;
- Security Control Point Date;
- Security Control Point Time;
- Security Control Point Location; and,
- Badge identification information including unique Badge Number for BEP SAC badge or the following fields to uniquely identify an individual using information from their PIV Card:
  - PIV Agency Code
  - PIV System Code
  - PIV Credential Number
  - PIV Credential Series
  - PIV Individual Credential Issue
  - PIV Person Identifier
  - PIV Organizational Category
  - PIV Organization Identifier
  - PIV Person Origination Associate Category
  - PIV Expiration Date

Other Federal government personnel and members of the public conducting business with the BEP, who have not undergone a formal security background clearance process and issued a Visitor Badge:

- Full name;
- Name of individual who they are visiting;
- Time, date, and location of each passage through a security control point; and
- Picture.

Individuals provided with SAC badges are required to provide:

- A U.S. Government/State/Territory issued picture identification; or
- A foreign issued passport.

BEP does not collect additional information or PII from individuals that require access to sensitive/restricted areas within BEP facilities. BEP uses the member's access profile to designate the areas where the individual is authorized to enter.

3. **Accuracy, Timeliness, and Reliability**

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

In the normal course, BEP receives the PII directly from the individual and considers the information accurate. BEP does not have an automated method for validating information submitted by third parties on behalf of individuals seeking access to BEP facilities. BEP employees may correct their information through the BEP HR Connect Portal. Individuals that are not BEP employees are required to resubmit accurate information prior to gaining access to BEP facilities or sensitive/restricted areas within BEP facilities.

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?**

BEP DCF Office of Security and WCF Security Division personnel conduct periodic data quality reviews to ensure that the data that they maintain is accurate.

d. **Are the data elements described in detail and documented? [ ] No [X]Yes**

If yes, what is the name of the document?

BEP procured the ISS System as a COTS acquisition. BEP reserves the rights to designate the data elements that are required to manage ID validation, authentication, and facility access. This PIA (Section 3. e. above) serves as documentation of the PII data elements required to best manage the ISS System. BEP may decide to use additional PII data elements based on growth of the system and will update this PIA should the need arise.

C. <u>Attributes of the Data</u>

1. **Is the use of the data both relevant and necessary to the purpose for which the system is being designed?**

Yes. The data collected is necessary to protect the security of BEP personnel and property by identifying and approving all physical access to the BEP facilities. BEP is a high security facility and is, in general, closed to the public. With the exception of limited area public tours that operate outside the auspices of this program and the ISS

System, access to BEP property is limited to BEP employees, contractors, service company employees, other U.S. Government agency employees, and members of the public conducting business with the BEP.

BEP employees, contractors, service company employees, other U.S. Government agency employees, and members of the public requesting access to BEP property may be required to present suitable identification, PII, and may be required to sign entry logs or registers before entering and existing the property.

BEP does not use this information for other purposes not associated with the physical access screening process.

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? [x] No [ ] Yes**

   Although the system tracks the movement of an individual through the building as they badge into or out of a controlled area within BEP property, it does not use this data to create new data or to aggregate the data in such a manner that would constitute datamining by developing predictive patterns or trends associated with the individual.

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

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

   No. Although the system can track the location of an individual through BEP when they enter or leave specific locations within BEP property, it does not use the data to conduct additional vetting against law enforcement databases or to make other decisions about individuals not associated with access to a BEP facility.

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

   This new data is not the result of analysis or created by fusing data from disparate sources. It is new information stored as the result of an event. It is relevant by definition, as this is the specific information the system was designed to acquire and store. The data is assumed to be accurate unless the underlying system is broken.

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

   BEP will not consolidate the data.

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

   BEP will not consolidate the processes associated with the data or the physical access security program.

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.**

   The data will be retrieved by personal identifier using the individual's First Name, Last Name, and Badge Number. BEP will also retrieve the information by Date, Badge Reader Device, Room Location, and specific Entry Location/Door. Treasury/BEP SORN 027 (ACAMS) provides coverage for this activity.

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

   Authorized personnel within the BEP Security Division can generate reports related to particular individuals and/or areas to identify attempts to access a facility or sensitive/restricted areas, date and time of the attempt, and whether access was granted or revoked. Additional reports are prepared to identify who was present in an area during a particular date or timeframe and the duration the individual(s) were in the area. The ISS System can also generate aggregate reports devoid of PII to assess access and security parameters throughout BEP facilities or sensitive/restricted areas.

D. 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?**

   BEP designed the ISS System in an IT architecture known as a "Three Node Cluster." The nodes within this cluster of systems serve as communication points between the systems that allow BEP to replicate the data on all systems within the cluster in real time. This configuration maintains a consistent copy of the data at all times.

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

   Official records, both electronic and hardcopy, relating to management and operation of BEP's security systems that monitor and protect employees and products, will be retained for five years or until no longer needed for reference, whichever is later. These records are retained and disposed of in accordance with the National Archives and Records Administration (NARA) approved BEP Records Retention and Disposal Schedule (N1-318-11-1).

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 procedures are documented in BEP Circular No. 80-05.4, *Policies and Procedures for Electronic Records and Email*, dated December 18, 2006. . Any reports produced are to be kept in accordance with the BEP Records Retention and Disposal Schedule (N1-318-11-1).

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.**

   Yes. Although PIV usage is not new, BEP will use it in association with physical access for the first time. The system uses GSA issued PIV cards. PIV data is used to validate user identities and for physical access.

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

   Members of the public attending tours within limited areas of BEP facilities are not participants in the ISS System or processes and are not impacted by this technology. The ISS System impacts the privacy of employees, contractors, and official visitors from other agencies or commercial companies by collecting PII from the individual and using it for the purpose of identity verification, authentication, and to grant or deny access to BEP facilities. Although BEP may use the technology to determine the whereabouts of individuals authorized to enter or transit within BEP facilities, it does not use the technology to predict patterns or trends associated with the individual or track their movements for reasons other than personnel/facility security. BEP operates the ISS System in accordance with the parameters set forth in Treasury/BEP SORN 027 (ACAMS). The SORN and this PIA serves as notice to the public on how BEP will use data associated with the ISS System.

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

   Yes, the ISS System performs ID verification and authentication and also monitors all individuals attempting to access BEP facilities and/or sensitive/restricted areas.

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

   The ISS System collects the date and time an individual enters and leaves specific areas at BEP. The ISS System can allow BEP Security Division personnel to determine the identity of individuals transiting within BEP facilities or sensitive/restricted areas when needed.

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

   The ISS System uses strict physical and logical access controls to limit access to approved BEP Security Division personnel that have a need to use the system in the performance of official duties. BEP personnel must be approved and cleared to access the locations where the system and information may be displayed. ISS users are also required to acknowledge and sign an IT Rules of Behavior agreement and complete annual mandatory Security Awareness Training and Privacy Awareness Training sponsored by the Department of the Treasury, Office of Privacy and Civil Liberties (OPCL).

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

   TREASURY/BEP .027 Access Control and Alarm Monitoring Systems (ACAMS), 78 Fed. Reg. 22604 (April 16, 2013).

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

    No

E. Access to Data

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

   Only BEP security personnel, authorized contractors, and IT system managers have access to ISS and its data.

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 ISS data. The BEP Active Directory is used to enforce a user's data access rights based on the roles they have been approved for.

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

   Authorized users have access to all data on the system. Access controls restrict functional capabilities of users not their access to the data.

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.**

   Authorized users must sign the IT System Rules of Behavior and complete the Annual Security Awareness Training and the mandatory Annual Privacy Awareness Training sponsored by the Department of the Treasury, Office of Privacy and Civil Liberties (OPCL) and the Records Management-Employees and Contractors Training sponsored by the Department of the Treasury, Office of Privacy, Transparency, and Records (OPTR). In addition, access to the information is strictly controlled by both physical and logical access and limited to an approved group of personnel. Approved personnel must be cleared for the rooms where the information may be displayed and be cleared to access the applications

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

   Yes. The system is a Commercial-Off-The-Shelf (COTS) product. If a problem is encountered, the vendor is brought in to troubleshoot and resolve the issue.

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

Yes. The ISS System can retrieve user ID verification data from the BEP Active Directory Network that maintains the identity of users authorized to access systems within the BEP IT Network.

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

   In the normal course, all personnel within BEP's Security Office that are authorized to access and/or manage PII contained in the ISS System are responsible for protecting the privacy rights of all individuals impacted by this system. Additionally, the Office of Critical Infrastructure and IT Security and the Privacy Office are also responsible for protecting the privacy of impacted individuals by establishing security and privacy compliance measures and documentation for the system.

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

   In the normal course, external agencies will not have automatic access to the ISS System or its data. BEP may share data with external entities pursuant to Routine Uses set forth in Treasury/BEP 027 (ACAMS) SORN, which is available at: https://www.treasury.gov/privacy/issuances/Documents/2013-08849.pdf.

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

   If BEP shares data with a third party in accordance with Treasury/BEP 027 (ACAMS) SORN, the receiving agency may use it in accordance with the Routine Use that triggered the information sharing requirement.

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

    The primary responsibility for proper ISS data use resides with the WCF–Manager, Security Division and the Chief, DCF Physical Security Division. Secondary responsibility resides with all authorized users of the ISS System.

The Following Officials Have Approved This Document