



**Department of the Treasury
Bureau of Engraving and Printing**

**Privacy Impact Assessment (PIA)
Western Currency Facility (WCF) Security
Systems – Integrated Security System (ISS)
and Data Acquisition System (DAS)**

**Office of Critical Infrastructure
and Information Technology Security
November 2006**

Section II

Bureau of Engraving and Printing Privacy Impact Assessment

A. System Information

1. What is the system name?

Western Currency Facility (WCF) Security Systems – Integrated Security System (ISS) [350104-ISS] / Data Acquisition System (DAS) [350102-DataAcquisition]

2. What is the purpose and intended use of this system?

This system allows the Western Currency Facility (WCF) to control access and monitor the movement of individuals entering and leaving the facilities and special areas within the facilities for purposes of maintaining physical and personal security and verification of employee attendance through review.

3. Does this system contain any personal information about individuals? (If no, a PIA is not required. Skip to Section III.)

Yes – The individual's name and photograph

4. What legal authority authorizes the purchase or development of this system/application? (List the statutory provisions or Executive Orders that authorize the maintenance of this information to meet an official program mission or goal)

5 U.S.C. 552a

5. For new systems, describe how privacy is addressed in documentation related to system development, including as warranted and appropriate, statement of need, functional requirements analysis, alternatives analysis, feasibility analysis, benefits/cost analysis, and especially, the initial risk assessment?

Not Applicable – The system is a legacy system without privacy aspects.

B. Data in the System

1. What categories of individuals are covered in the system? (e.g. employee, contractor, public)

Employees, contractors and visitors.

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

a. Is the information collected directly from the individual or is it taken from another source? If information is not collected directly from the individual, describe the source of the information.

Contact information in the system is obtained from other BEP systems that are established as part of the Personal Identity Verification (PIV) system. Credential numbers are obtained from the Video Badge Computer (VBC).

b. What Federal agencies provide data for use in the system?

Bureau of Engraving and Printing

c. What State and Local agencies provide data for use in the system

None

d. What other third parties will data be collected from?

None

e. What information will be collected from the employee and the public? (Be as specific as possible. List personal information collected from the public such as social security number, address, credit card number, telephone number. Employee information may include badge number, user identifier, telephone number, social security number, and health information.)

Employees and contractors provide their photo, name, work phone number, badge number, BEP access level, date PIV card issued, date PIV card expires and assorted other data concerning their employment at the Bureau.

Visitors (Public) provide only their names.

3. How does the Bureau ensure that data is sufficiently accurate, relevant, timely, and complete to ensure fairness in making determinations about any individual?

a. How is data accuracy ensured?

Information is provided as part of the individuals background check. Information is validated through cross referencing through data bases and identification check. The individual is required to submit the information within a specified time frame.

b. How will data be checked for completeness?

Data will be checked by computer application (EQIP) and verified by a staff member.

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

No. There is no regular process for up-dating the data except when the 5 year background investigation is performed.

d. Are the data elements described in detail and documented? If yes, what is the name of the document?

Yes. Vendor documentation is available that describes the user interface fields and their purpose.

e. How will data collected from sources other than BEP records be verified for accuracy?

Not Applicable. Data from non-BEP records is not utilized in the system.

4. Describe what opportunities individuals have to decline to provide information (i.e., where providing information is voluntary) or to consent to particular uses of information (other than required or authorized uses), and how individuals can grant consent.)

Individual consent to the use of their information when they apply for employment or access to a BEP facility.

C. 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?

Yes

2. Will the system derive new data or create previously unavailable data about an individual through the aggregation of information collected? (if no, skip to D.3)

Yes

a. Will the new data be placed in the individual's record?

No

b. Can the system make determinations about employees or the public that would not be possible without the new data?

Yes

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

The system has the ability to create the new data when an individual's badge is passed through a check point reader. If the system works as designed no verification is required.

3. Do the records in this system share the same purpose, routine use, and security requirements?

Yes, the system is used to track, control, and monitor access to facilities and sensitive areas and to verify an individuals presence in the facility to reconcile T &A records with pay and to investigate illegal activities.

a. If the data is being consolidated, what technical, management, and operational controls are in place to protect the data from unauthorized access or use? Explain

Data consolidation is not being implemented.

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

Process consolidation is not being implemented.

4. How will the data be retrieved? Can a personal identifier be used to retrieve data? Are personal identifiers used to retrieve data on a routine, occasional, or ad-hoc basis? If yes, explain and list the identifiers what will be used to retrieve information on the individual.

Data will be retrieved through inquiries resulting in reports. Personal identifiers can be used to retrieve data. Yes, on a routine basis. The name of an individual or badge number are the most frequently used identifiers, but one can also ask for all supervisors, persons with a certain level of security clearance, persons from a particular office or all persons who have passed a particular check point on a certain date and time.

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

Reports can be generated by authorized personnel within the Security Division on individuals and areas to identify who attempted to access a facility or sensitive/restricted areas, when the attempt was made, and if access was granted or rejected. Additional reports are prepared to identify who was present in an area on a particular date or during a particular timeframe and how long they were in the area. Other administrative reports can be printed to indicate who has access to an area, who has a particular level of clearance and frequency of access. The reports are used to monitor and control the security of the facilities and review attendance. Anyone who has a need to know from the individual involved and the individual's supervisor to the, Security Division and the Compliance Division.

D. Maintenance of Administrative Controls

1. If the system is hosted and/or used at more than one site, how will consistent use of the system and data be maintained at all sites?

The system is not hosted in multiple locations.

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

The data is to be retained for the life of the system. Currently, the Security Division conducts backups of the Data Acquisition System and has retained data since the implementation of the system (1995).

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?

Data will be destroyed when the system is ended.
Reports are retained for various periods of time determined by the office receiving the report. Account access update reports are updated every 6 months and maintained in the Physical Security Branch.
Procedures are documented in the Bureau Records Schedule.

4. Is the system using technologies in ways that the BEP has not previously employed (e.g. monitoring software, Caller-ID)? If yes, how does the use of this technology affect public/employee privacy?

No

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

Yes, the system monitors personnel attempting to access facilities and sensitive/restricted areas.

a. What kinds of information are collected as a function of the monitoring of individuals?

Date and time an individual enters and leaves specific areas.

b. What controls will be used to prevent unauthorized monitoring?

The Security Division has the ability to create a variety of reports.. Specified individuals in that division are given access to the system and are required to sign the BEP Rules of Behavior document and complete annual security awareness and privacy training. The system is housed in an area controlled by a badge system and password protection is provided for access to the computers.

6. Under which Privacy Act systems of records notice does the system operate? Provide name and number.

This system is not a Privacy Act system of records, but if it were it would operate under the notice identified as:

Access Control and Alarm Monitoring Systems (ACAMS) Treasury/ BEP .027

7. If the system is being modified, will the Privacy Act system of records notice require amendment of 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, other)

BEP employees and contractors working for the BEP Security Division and Compliance Division.

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

Only personnel involved with the monitoring or management of access controls are granted access to the system. Procedures for requesting and approving access are provided in the system security plan.

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 system rules of behavior and all users are required to complete annual security awareness and privacy training.

5. Are contractors involved with the design and development of the system and/or will they be involved with the maintenance of the system? (If yes, were Privacy Act contract clauses inserted in their contracts and other regulatory measures addressed?)

Yes. A contract clause was included in the contract.

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

No.

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

The Security Division Manager and the Compliance Division Manager.

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

Yes. The data may be shared with other agencies such as the Department of the Treasury, OIG and The United States Secret Service.

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

Generally, for investigative matters.

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

The Security Division Manager and the Compliance Division Manager.

SECTION III

Privacy Impact Analysis

System of Records Identification

1. Is a system of records being created under the Privacy Act, 5 U.S.C. 552a. If no, skip questions 2 through 4.

No

2. Have privacy and IT risk assessments been conducted that consider: the alternatives to collection and handling as designed, and the appropriate measures to mitigate risks identified for each alternative?

Risk assessments have been conducted as part of the certification and accreditation process.

3. What impact will this system have on an individual's privacy? (Consider the consequences of collection and flow of information and identify and evaluate threats to individual's privacy.)

The only personal information maintained in the DAS is the individual's name and photograph.

4. As a result of the PIA what choices have been made regarding the IT system of collection of information? Have adequate measures been designed and implemented to mitigate risk? What is the rationale for the final design choice or business process?

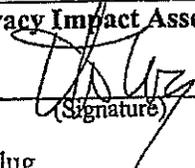
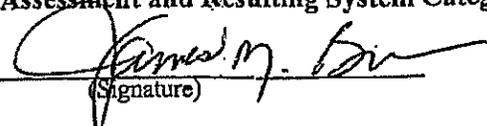
It was determined that imputing individual social security account numbers was not necessary. Therefore, all SSNs were removed from the database. Adequate measures have been implemented to protect the minimal amount of personal data maintained within the system.

Section IV

System Development Lifecycle Privacy Requirements Worksheet

A. Contact Information	
1. Person who completed the Privacy Impact Assessment document	
Name:	Thomas Klug
Title:	Manager
Organization:	Security Division, Western Currency Facility
Phone number:	(817) 847-3927
2. System Owner	
Name:	Thomas Klug
Title:	Manager
Organization:	Security Division, Western Currency Facility
Phone number:	(817) 847-3927
3. IT Security Reviewer	
Name:	Harry Singh
Title:	Division Manager
Organization:	IT Security Division
Phone number:	(202) 874-0003
4. Bureau Privacy Reviewer	
Name:	James Braun
Title:	Privacy Officer
Organization:	Office of Chief Counsel
Phone number:	(202) 874-3733

Privacy Impact Assessment Summary		
System Category (check all categories that apply)		Requirement
N/A	System of Records	Publish System of Records Notice
N/A	Website available to the public	Publish Privacy Impact Assessment
N/A	Website or information system operated by a contractor on behalf of the Bureau for the purpose of interacting with the public	Publish Privacy Impact Assessment
N/A	New or significantly altered information technology investment administering information in an identifiable form collected from or about members of the public	Conduct Privacy Impact Assessment
N/A	New or significantly altered information technology investment administering information in an identifiable form collected from or about Bureau employees	
N/A	Contains medical information	Determine if system is subject to HIPAA
X	Other: Legacy System with personal information	Conduct Privacy Impact Assessment
	None of the above	Privacy Impact Assessment not required

Privacy Impact Assessment Approval	
Approval of Privacy Impact Assessment accuracy and completeness.	
System Owner: <u></u> (Signature)	<u>11/14/06</u> (Date)
Name: Thomas Klug Title: Manager, Physical Security Branch	
Approval of IT System Risk Assessment	
Manager, IT Security Division: <u></u> (Signature)	<u>03-17-07</u> (Date)
Name: Harry Singh Title: Manager, IT Security Division	
Approval of Privacy Assessment and Resulting System Category	
Privacy Act Officer: <u></u> (Signature)	<u>3/16/07</u> (Date)
Name: James Braun Title: Privacy Officer	