Department of the Treasury
Bureau of Engraving and Printing

Privacy Impact Assessment (PIA) Technical Security Division (TSD) Security Systems – Access Control Alarm Monitoring System (ACAMS)

Office of Critical Infrastructure
and Information Technology Security
April 2006

Section II

Bureau of Engraving and Printing Privacy Impact Assessment

A. System Information
1. What is the system name? Technical Security Division (TSD) Security Systems – Access Control Alarm Monitoring System (ACAMS) [520123-ACAMS]
2. What is the purpose and intended use of this system? This system is used for access control and to monitor the alarm intrusion End of Line (EOL) devices for the Washington, D.C. facility. The access control system feature enables BEP to strictly control when an authorized employee accesses the facility and their assigned work area(s).
3. Does this system contain any personal information about individuals? (If no, a PIA is not required. Skip to Section III.) Yes – identifying numbers or symbols assigned to the individual as well as names, and contact information.
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

B. Data in the System
1. What categories of individuals are covered in the system? (e.g. employee, contractor, public) Employees and contractors

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 System (VBS).

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.).

Photograph; Full name; Social Security number; date of birth; badge number; supervisory status, work telephone; work area number; BEP access clearance level; date BEP access level granted; date last security background investigation was completed; BEP access level; BEP access time zone; date access badge issued; date access badge voided; time, date and location of each passage through a security control point.

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 provided by Personnel Security Division (PSD).

b. How will data be checked for completeness?

Data is checked by PSD.

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 What steps or procedures are taken to ensure the data is not out-of-date?

The information is updated during the 5 year background investigation.

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

The system is a Commercial-Off-The-Shelf (COTS) product. Vendor documentation was provided 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)

No

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

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

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

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

Yes, the system is only used for the creation and management of individual credentials.

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.

Authorized system users must positively identify and authenticate themselves to the system before being granted access to the information.

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 Office of Security 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 revoked. 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.

D. Maintenance of Administrative Controls
1. If the system is hosted and/or used at more that 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? 5 Years.
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? Account Access Update Reports are updated every 6 months and destroyed after 6 months.
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? Users are required to sign a rules of behavior and complete annual security awareness training.
6. Under which Privacy Act systems of records notice does the system operate? Provide name and number. BEP .027
7. If the system is being modified, will the Privacy Act system of records notice require amendment of revision? Explain. System is not being modified at this time.

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 Office of Security Technical Security 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 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? 5 U.S.C. § 552a(m)
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? Not Applicable.
8. Will other agencies share or have access to the data in this system? If yes list agencies. No.
9. How will the data be used by the other agency? Not Applicable.

10. Who is responsible for assuring proper use of the data? Not Applicable.

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? N/A
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.) N/A
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? N/A

Section IV

System Development Lifecycle Privacy Requirements Worksheet

A. Contact Information
1. Person who completed the Privacy Impact Assessment document Name: Richard Hoppe Title: Security Specialist Organization: Office of Security, TSD Phone number: 202.874.3448
2. System Owner Name: Debra Etkins Title: Manager, Technical Security Division Organization: Office of Security Phone number: (202) 874-4020
3. IT Security Reviewer Name: : Harry Singh Title: Manager, IT Security Division Organization: Critical Infrastructure & IT Security Phone number: : (202)874-0003
4. Bureau Privacy Reviewer Name: Jim 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
X	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: _____ (Signature) 5/23/07 (Date)

Name: Debra Etkins
Title: : Manager, Technical Security Division

Approval of IT System Risk Assessment

Manager, IT Security Division: _____ (Signature) 05-22-07 (Date)

Name: Harry Singh
Title: Manager, IT Security Division

Approval of Privacy Assessment and Resulting System Category

Privacy Act Officer: _____ (Signature) 5/24/07 (Date)

Name: Jim Braun
Title: Privacy Officer