Pension Benefit Guaranty Corporation

Information Technology Infrastructure Operations Department (ITIOD)

Physical Access Control & Surveillance System (PACSS) Privacy Impact Assessment (PIA)

Last Updated: 07/17/2025

1 PRIVACY POINT OF CONTACT

Name	Catherine Diamante
Title	Information System Security and Privacy Officer (ISSPO)
Phone	202.229.6039
Email	Diamante.catherine@pbgc.gov

2 PRIVACY IMPACT ASSESSMENT

A Privacy Impact Assessment (PIA) is an analysis of how information is/will be handled:

i. To ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy,
ii. To determine risks and effects of collecting, maintaining, and disseminating information in an identifiable form in an electronic information system, and
iii. To examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

Privacy concerns are highest for systems that contain Personally Identifiable Information (PII). PII is defined as information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. Because there are many types of information that can be used to distinguish or trace an individual's identity, the term PII is necessarily broad.

TIP!

Information that either alone or when considered with other information that uniquely identifies a person is Personally Identifiable Information (PII). Combining pieces of information whether private or publicly available has powerful implications for uniquely identifying an individual.

For example, consider a person named Mary Jones. There are over 200 million results in an internet search for this name. But if we combine information such as a date of birth, the last four digits of a (or worse, an entire) Social Security Number, or a spouse's name, the number of persons to whom we could be referring begins to narrow quite rapidly. These types of information are considered identifiers. Identifiers that uniquely identify a person are the focus of privacy protection.

2.1 The Components of the System

Name of component	Describe the component (1 or 2 sentences)	Does this component contain PII	In what system of records (SORN) is this information stored	What is the Legal Authority for collection of this information	Does this system share PII internally *(please detail in question 9)*
C.CURE 9000 SECURITY MANAGEMENT SYSTEM	C.Cure 9000 is a security management system that provides physical access controls including card readers and servers for auditing purposes. Credentials and clearances are verified by C.Cure 9000, access to the PBGC facility is then approved.	Yes	PBGC-28, Physical Security and Facility Access	Executive Order 12977; 6 CFR part 37; Homeland Security Presidential Directive (HSPD) 12: Policy for a Common Identification Standard for Federal Employees and Contractors.	Yes
BOSCH VIDEO MANAGEMENT SYSTEM (BVMS)	Bosch Video Management System (BVMS) uses IP-enabled cameras to monitor personnel movements throughout the PBGC. Security guards and other authorized PBGC personnel are able to view camera feeds in real time or from archives.	Yes	PBGC-28, Physical Security and Facility Access	Executive Order 12977; 6 CFR part 37; Homeland Security Presidential Directive (HSPD) 12: Policy for a Common Identification Standard for Federal Employees and Contractors.	Yes
TRAKAeKEY MANAGEMENT SYSTEM (TRAKA)	Traka Key Management is used to store and manage physical keys, and to control key issuance to authorized users only. Traka secures,	Yes	PBGC-28, Physical Security and Facility Access	Executive Order 12977; 6 CFR part 37; Homeland Security Presidential Directive (HSPD) 12:	Yes

Name of component	Describe the component (1 or 2 sentences)	Does this component contain PII	In what system of records (SORN) is this information stored	What is the Legal Authority for collection of this information	Does this system share PII internally *(please detail in question 9)*
	manages, and audits the use of every key. Traka web integrates with C.Cure 9000 for centralized access management.			Policy for a Common Identification Standard for Federal Employees and Contractors.	

2.2 The System as a Whole

1. Please describe the purpose of the system when considered as a whole.

The Physical Access Control and Surveillance System (PACSS) manages and monitors physical access to PBGC facilities by employees, contractors, and visitors. PACSS grants access through queries to Active Directory based on information obtained from individual Personal Identity Verification (PIV) cards for employees and contractors, and records verification of visitors through off-line proof of identity. PACSS also monitors physical movements throughout the facility and enables real-time viewing and archival retrieval for security guards and other authorized personnel. PACSS is a FISMA Child of the parent ITISGSS and is not FISMA reportable.

2. What are the Confidentiality, Availability, and Integrity ratings for the system as a whole?

Confidentiality	Moderate
Integrity	Moderate
Availability	Moderate

3. Is this a contractor system?

☒Yes
☐No

4. Is this a new or existing information system? If this is an existing information system, please describe the changes.

This is an existing information system and there have been no changes.

5. Does your system collect, process, or maintain any records that describe how any individual exercises their First Amendment rights?

   If so, please describe the information it collects and the purpose for the collection. Please describe whether: 1) an express legal authority authorizes the collection, 2) the collection is pertinent to and within scope of an authorized law enforcement activity, or 3) the individual(s) consents to the collection.

   (The First Amendment guarantees an individual's right to the exercise of their religious beliefs, their petitioning the government, their exercise of free speech, their right to peaceably assemble, and the freedom of the press.)

The system does not collect, process, or maintain any records that describe how any individual exercises their First Amendment rights.

6. For the PII in the system, discuss the actual/intended uses of the PII; procedures taken to limit the PII collected to the minimum needed; reasons the PII is necessary and relevant; and procedures taken to periodically review the accuracy, relevance, timeliness, and completeness of PII throughout the information life cycle.

The PII is used to grant physical access to PBGC employees and contractors by authenticating PIV credentials, and to visitors by examining identification documents (e.g., driver's license, passport). PII is needed to provide a robust Physical Access Control & Surveillance System. PACSS also monitors physical movements throughout the facility and enables real-time viewing and archival retrieval for security guards and other authorized personnel. PBGC does not collect audio through its cameras, cameras are directed in a manner to minimize views of any screens, we retain video recordings according to the records schedule and only collect the PII needed for badging and movement throughout the facility needed to maintain a secure workplace.

7. Discuss how your system retrieves PII. Please describe the identifiers used to locate records within a system, such as name, identification number, date of birth, etc.

The system uses first and last name identifiers to locate records within PACSS.

8. Approximately how many individuals' PII is maintained in the system?

Approximately 2,300 records are maintained in the system.

9. Is the submission of PII by individuals voluntary or mandatory? If the submission is voluntary, what is the outcome of an individual not submitting PII.

The submission of PII by individuals is mandatory.

10. If your system collects Social Security Numbers:

    a. Please provide a justification for the collection, use, maintenance, and disposal of PII in the form of SSN?

    The PACSS system does not collect use, maintain, or dispose PII in the form of SSNs

    b. Under which authorized uses, as described in the "Reduction of use of Social Security Numbers (SSN) in PBGC" policy document?

Not Applicable

c. If the answer to b., above is "Compelling Business Need," please provide a plan to reduce the use of SSNs, highlighting activities that can be completed in the next 12 months.

Not Applicable

11. List and discuss the sources from which the system collects PII (for instance, from an individual, another federal agency, etc.); the format in which PII is collected (for instance, via a form, face-to-face, phone, etc.); the notification given at time of collection from an individual regarding the Privacy Act and the ability to opt-out of collection (and the consequences of opting out). Include a copy of all forms and Privacy Act statements used to collect information.

For PBGC employees and contractors, PII is imported from PBGC Active Directory. Visitor information is collected from the government-issued identification that is presented when they check-in. The format for collecting PII is by electronically authenticating PIV credentials, temporary access card numbers, access clearance, key number, key removal date and time, and visitor credentials at the time of visit. Individuals are notified of the collection of PII through the PBGC Privacy Act Statement

12. Discuss any privacy controls that PBGC inherits from an external provider (cloud provider, third party provider, another government agency, etc.) If an Interconnection Security Agreement (ISA), Memorandum of Understanding (MOU), or similar document is in place, please summarize the privacy applicable portions of that document.

Physical Access Control and Surveillance System (PACSS) does not inherit any privacy controls from any external service provider.

13. Is the PII shared with external (non-PBGC) organizations? If so, identify with whom the PII is shared and the purpose. Discuss the data flows within the system (include sources of data for data flowing into the system, destinations for data flowing out of the system, and any routine uses applicable to the system). For any information that is shared internally, be sure to discuss whether these data interconnections are noted in CSAM. Be sure to include any MOU, ISA, or Interagency Agreements.

The PIV FASC_N, which contains the legal names and email addresses of employees and contractors, is shared with Datawatch Systems, so our employees can access the main lobby doors after-hours. PBGC does not control door access for the main lobby doors, so we provided Datawatch with an Excel spreadsheet with all the active employees FASC_N. The FASC_N is one of the primary identifiers on the PIV Card for physical access control, as required by FIPS 201. The FASC-N is a fixed length (25 byte) data object that is specified in [NIST SP 800-73-4] and included in several data objects on a PIV Card. We are covered by SORN-28 to provide this information to an external organization.

14. For the user roles in the system:

Role Name	Number of Users in that Role	Approver	Access Level (Read, Write, etc.)	Recertification Date
APPS_Bosch_BVMS_ Operator	34*	Approved by Supervisor & Service Owner(s)	This role has limited read-only access to the C.CURE 9000 Monitoring and Administration clients. Access is role-based and is based on ACLs needed to perform non-privileged duties as assigned	6/20/2025
Apps_CyberArk_prdw-bvms-admin (apsvc510/511)	4*	Approved by Supervisors & Service Owner(s)	Access is role-based and is based on ACLs needed to perform privileged duties as assigned. This includes network, system, & database administrators.	6/20/2025
APPS_SoftwareHouse_CCure9000_FPS	15*	Approved by Supervisor & Service Owner(s)	This role has limited read-only access to the C.CURE 9000 Monitoring and Administration clients. Access is role-based and is based on ACLs needed to perform non-privileged duties as assigned.	6/20/2025
APPS_SoftwareHouse_CCure9000_Physical Security	10*	Approved by Supervisor & Service Owner(s)	This role has read-only access to the C.CURE 9000 Monitoring and Administration clients. Access is role-based and is based on ACLs needed to perform	6/20/2025

Role Name	Number of Users in that Role	Approver	Access Level (Read, Write, etc.)	Recertification Date
			non-privileged duties as assigned.	
Apps_CyberArk_prdw-pacss-admin **(apsvc613/614)**	4*	Approved by Supervisor & Service Owner(s)	This role gives access to the CyberArk safe to broker apsvc613/apsvc614 accounts which are ROLE - CyberArk PACSS Administration. Access is role-based and is based on ACLs needed to perform privileged duties as assigned. This includes network, system, & database administrators.	6/20/2025
Apps_CyberArk_prdw-traka-admin **(apsvc291/292)**	4*	Approved by Supervisor & Service Owner(s)	This role gives access to the CyberArk safe to broker apsvc291/apsvc292 accounts which are Rolee CyberArk Traka Administration Access is role-based and is based on ACLs needed to perform privileged duties as assigned. This includes network, system, & database administrators.	6/20/2025

15. Discuss the Physical, Technical, and Administrative controls that are employed to secure the PII in the system.

Physical Controls - Physical security controls employed to secure the PII in the system include:*

- *Physical Access Authorizations*
- *Physical Access Control*
- *Access Control for Transmission Mission*
- *Access Control for Output Devices*
- *Monitoring Physical Access*
- *Visitor Control*
- *Access Records*
- *Power Equipment and Power Cabling*
- *Emergency Shutoff*
- *Emergency Power*
- *Emergency Lighting*
- *Fire Protection*
- *Temperature and Humidity Controls*
- *Delivery and Removal*
- *Alternate Work Site*
- *Location of information Components*
- *Information Leakage*

*

Technical Controls - Technical controls employed to secure the PII in the system include:*

- *Account Management*
- *Access Enforcement*
- *Authenticator Management*
- *Cryptographic Module Authentication*
- *Information Flow Enforcement*
- *Separation of Duties*
- *Least Privilege*
- *Unsuccessful Login Attempts*
- *Remote Access*
- *Wireless Access*
- *Audit Events*
- *Audit Review, Analysis, and Reporting*
- *Time Stamps*
- *Audit Record Retention*
- *Non-repudiation*
- *Session Audit*
- *Public Key Infrastructure Certificates*

- *Denial of Service*
- *Network Disconnect*
- *Session Authenticity*
- *Protection of Information at Rest*

Administrative Controls - All PBGC users are required to complete privacy training annually. Administrative controls employed to secure the PII in the system include:

- *Periodic Security Audits*
- *Regular Monitoring of User's Activities*
- *Annual Security, Privacy, and Records Management Refresher Training*
- *Backups Secured Offsite*
- *Encryption of Backups containing sensitive data*
- *Role-Based Training*
- *Least Privilege Access*
- *Mandatory on-boarding training for security, privacy, and Records management personnel*

16. Please discuss additional training for users, other than the PBGC mandatory annual training, for protecting information in the system.

No additional training provided for users

17. Does the System leverage the Enterprise Access Controls?

☒ Yes
☐ No

18. Does the system leverage the commonly offered control for Accounting of Disclosures?

☒ Yes
☐ No

19. Discuss the process in place for retention and destruction of PII. Cite the applicable retention schedule(s).

Key and Card Access Accountability Records:
These records are destroyed after 6 months. In C-CURE, they are automatically purged from reporting after 12 months.
Reference: GRC 5.6, Item 121

Visitor Processing Records:
Retained for 5 years, after which they are destroyed. Longer retention is permitted if required for business purposes.
Reference: GRS 5.6, Item 110

Facility Security Management Operations Records:
Destroyed after 30 days, unless extended retention is needed for business use.

- *Surveillance video recordings are retained for 60 days - In BVMS (within PACSS), the retention period is configured for 60 days, which exceeds the General Records Schedule (GRS) requirement and aligns with business needs.*
- *GRS 5.6 recommends a temporary retention period of 30 days.*
  Reference: GRC 5.6, Item 090

Access Activity Reports:
C-CURE 9000 retains access activity data for up to 12 months, beyond which queries cannot be performed. However, access activity logs are continuously forwarded to CACM. Within CACM, the data is retained for 3 years before being archived; once archived, it remains stored indefinitely. Currently, there is no data destruction policy in place.

GRS 5.6: Security Management Records

2.3 Privacy Office Review

Name of Reviewer	Corey Garlick
Date Reviewed	7/17/2025
Expiration Date	7/17/2026
Result	☒ Approved without conditions ☐ Approved with conditions (see below). ☐ Denied

(For Privacy Office Use Only)

Discuss analysis of risks and compensating controls (or other mitigation steps).

Enter description here.

Discuss any conditions on Approval
