Pension Benefit Guaranty Corporation

Information Technology Infrastructure Operations Department (ITIOD)

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

Last Updated: 05/30/2024

1 PRIVACY POINT OF CONTACT

Name	Lester Hockman
Title	Information System Security and Privacy Officer (ISSPO)
Phone	202.286.3879
Email	hockman.lester@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.

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 control 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 archive.	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
TRAKA KEY 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, manages, and audits the use of every key. Traka web integrates with C.Cure 9000 for centralized access management.	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

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)*
Microsoft SQL Databases	A PaaS engine that handles database functions as such upgrading, patching, backups, and monitoring without user involvement	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

2.2 The System as a Whole

1. Please describe the purpose of the system, when considered as a whole, please include if this is an existing system (either an annual recertification update or a major change).

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 is the Confidentiality, Availability, and Integrity ratings for the system as a whole?

Confidentiality	Moderate
Integrity	Moderate
Availability	Moderate

3. 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, visitor name, Photo, date and time of visit, organization, name of PBGC personnel escorting the visitor, visitor badge number and reason for visit. PII collected from employees and contractors include Name, Email Address, Phone Number, Photos, and physical movements (key entry and video recordings).

4. 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.

5. 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 in ACLs needed to perform non-privileged duties as assigned	5/14/2024
Apps_CyberArk_prdw-bvms-admin (apsvc510/511)	4*	Approved by Supervisors & Service Owner(s)	Access is role-based and is based in ACLs needed to perform privileged duties as assigned. This includes network, system, & database administrators.	5/14/2024
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 in ACLs needed to perform non-privileged duties as assigned.	5/14/2024
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 in ACLs needed to perform non-privileged duties as assigned.	5/14/2024
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 in ACLs needed to perform privileged duties as assigned. This includes network, system, & database administrators.	5/14/2024
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 Role -	5/14/2024

Role Name	Number of Users in that Role	Approver	Access Level (Read, Write, etc.)	Recertification Date
			CyberArk Traka Administration Access is role-based and is based in ACLs needed to perform privileged duties as assigned. This includes network, system, & database administrators.	

*Account membership as of 5/14/2024

6. Does the System leverage the Enterprise Access Controls?

☒ Yes
☐ No

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

- *Physical Controls - Entrance to PBGC HQ facilities employ armed guards and a PIV activated turnstile. Most rooms on the 1st and 2nd floors and selected office suites throughout the upper floors require a PIV for physical access. Physical security controls employed to secure the PII in the system include:*
  - *Security Guards*
  - *Secured Facility*
  - *Key Entry*
  - *Identification Badges (PIV)*
  - *Locked Offices*
  - *Locked File Cabinets*
- *Technical Controls - Technical controls employed to secure the PII in the system include:*
  - *Access Enforcement*
  - *Information Flow Enforcement*
  - *Least Privileges*
  - *Data Encryption*
  - *System Use Notification*
  - *Session Lock*
  - *Personal Identity Verification (PIV) card access*
  - *Session Termination*
  - *Remote Access*
  - *Time Stamps*
  - *Identifier Management*
  - *Authenticator Management*
- *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*
- *Visitor Access Records*
- *Mandatory on-boarding Training*
- *Records Management*

8. For the PII in the system, discuss the actual/intended uses of the PII; the steps taken to limit the PII collected to the minimum needed; and the reasons the PII is necessary and relevant.

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.

9. 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.

Card readers obtain information from PIV cards and forward that data to the C.CURE management server. C.CURE software on the management server queries Active Directory for authentication verification and access authorization, then sends a command to the turnstile or door lock to allow access. For visitors, name, pictures, reason for visit, organization name, date and time of visit, floor being visited is manually checked by security personnel and recorded on a security log.

BVMS cameras located throughout the facility send video streams to video recorders as directed by the BVMS management server. Designated workstations manned by authorized users access the video streams via the management server which retrieves the needed stream from the video recorder.

Physical keys to offices and other controlled spaces are stored in IP-enabled key cabinets located throughout the facility. Requests for key issuance are sent to the Traka management server which queries Active Directory for authorization and then sends a command to the appropriate key locker to dispense the requested key.

Data flows into the PACSS system from PIV cards and Active Directory. All data flows between PACSS components are encrypted in transit.

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

☒ Yes
☐ No

11. 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

2.3 Privacy Office Review

Name of Reviewer	Margaret Drake
Date Reviewed	5/30/2024
Expiration Date	7/30/2024

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

I recommend that the Chief Privacy Officer approve this PIA for 2 months at which time Privacy and IT will update the data flow and roles for the SQL server.