Pension Benefit Guaranty Corporation

Information Technology Infrastructure Operations Department (ITIOD)

CDM – CrowdStrike Privacy Impact Assessment (PIA)

Last Updated: 09/16/2025

1 PRIVACY POINT OF CONTACT

Name	Catherine Diamante
Title	Information System Security and Privacy Officer (ISSPO)
Phone	202-403-4260
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)*
CrowdStrike Falcon Agent	CrowdStrike Falcon is a sensor installed on all PBGC Government-Furnished Equipment (GFE) laptops and servers. The Falcon sensor, installed on laptops and servers, blocks attacks and continuously monitors system activities like processes, network traffic, and file access.	Yes	PBGC - 26: PBGC Insider Threat and Data Loss Prevention	29 U.S.C. 1302(b)(3); 5 U.S.C. 301; 44 U.S.C. 3101; 44 U.S.C. 3554; Executive Order 13587, Executive Order 3356, Controlled Unclassified Information; 5 C.F.R. 731; 5 C.F.R. 302; OMB Circular A-130	Yes
CrowdStrike Falcon Cloud Platform	This Software as a Service (SaaS) solution enables PBGC to identify unknown malware, detect zero-day threats, identify advanced adversaries, and prevent damage from targeted attacks in real-time.	Yes	PBGC - 26: PBGC Insider Threat and Data Loss Prevention	29 U.S.C. 1302(b)(3); 5 U.S.C. 301; 44 U.S.C. 3101; 44 U.S.C. 3554; Executive Order 13587, Executive Order 3356, Controlled Unclassified Information; 5 C.F.R. 731; 5 C.F.R. 302; OMB Circular A-130	Yes

2.2 The System as a Whole

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

CrowdStrike Falcon Platform *is a Software as a Service (SaaS) solution, as defined by the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-145. It leverages Amazon Web Services (AWS) GovCloud to deliver a secure and FedRAMP compliant architecture. This SaaS solution enables PBGC to identify unknown malware, detect zero-day threats, identify advanced adversaries, and prevent damage from targeted attacks in real-time. By storing and analyzing vast amounts of event data in a scalable elastic cloud, CrowdStrike identifies targeted attacks in real-time. CrowdStrike is Federal Information Security Modernization Act (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 system and there are currently 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.)

No

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 data collected is used for user identification, audit trails, and policy enforcement (for specific user groups). Access to PII information is limited only via authorized personnel who are added to the restricted entitlement group.

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.

CrowdStrike Falcon does not directly collect traditional PII such as name, Social Security number, or date of birth; instead, it gathers system and telemetry data (e.g., device ID, hostname, IP address, user account names, email address and machine identifiers) that can indirectly link to individuals. These identifiers serve as keys to locate and correlate records within Falcon's system, allowing analysts to tie security events to specific endpoints or user sessions without storing sensitive personal attributes like DOB or government IDs

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

2,400

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 data is collected involuntarily, as it is an inherent part of the login and data collection process required for applying CrowdStrike to workstations. Sharing this information is necessary to enable proper functionality.

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?

Not Applicable

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.

CrowdStrike collects PBGC employees and contractors information, directly from the laptop or server in question. All PBGC devices provide a notice upon use of the device that data is collected. There is no functionality to opt-out as the function of the data collected is to ensure the security of the device and PBGC network.

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.

PBGC does not inherit privacy controls from any external 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.

CrowdStrike Falcon Agent: *CrowdStrike Falcon Agent is the sensor installed on all PBGC Government-Furnished Equipment (GFE) laptops and servers. The Falcon sensor, installed on laptops and servers, continuously monitors system activities like processes, network traffic, and file access. This log data, including any relevant metadata and minimal PII necessary for threat detection, is securely encrypted and transmitted to the CrowdStrike Falcon Cloud Platform via Transport Layer Security (TLS). Once in the CrowdStrike Falcon Cloud Platform, the data is analyzed using advanced algorithms, behavioral analysis, and threat intelligence to detect and respond to potential threats in real-time. The results are then made available through the Falcon platform's dashboard for security teams to take appropriate action. Then Cybersecurity and Infrastructure Security Agency (CISA) has the*

integration between CrowdStrike and Elasticsearch and Kabana for updating endpoint information for the CDM Agency and Federal Dashboards.
Addendum 3 to the Memorandum of Agreement (MOA) between the Cybersecurity and Infrastructure Security Agency (CISA) and PBGC is an ISA for the Continuous Diagnostics and Mitigation (CDM) Capability Shared Service Platform (SSP) 2.0.

14. For the user roles in the system:

Role Name	Number of Users in that Role (AD)	Approver	Access Level (Read, Write, etc.)	Recertification Date
APPS_DHS_CDM_AgencyDashboardToolUser (Privileged role)	16	Joe Sweeney, Hiep Vo	Read/Write	June 17, 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*

**Physical Controls are provided by both PBGC and the Cloud Service Provider (CSP)*

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*

***Technical Controls are provided by both PBGC and the CSP*

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.

Security Operations (SecOps) team is subject to CDM CrowdStrike training when accessing the CS console

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).

GRS 5.6: Security Management Records; 240 – Insider Threat User Activity Monitoring (UAM) Data - Destroy no sooner than 5 years after inquiry has been opened, but longer retention is authorized if required for business use.

ITIOD: CrowdStrike audit logs are stored in Splunk. The ingested data is searchable for 2 years and archived for an additional 4 years.

2.3 Privacy Office Review

Name of Reviewer	Duane Dodson
Date Reviewed	9/16/2025
Expiration Date	9/16/2026
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
