Pension Benefit
Guaranty Corporation

Information Technology Infrastructure Operations Department (ITIOD)

Continuous Diagnostics and Mitigation (CDM) - CrowdStrike Privacy Impact Assessment (PIA)

Last Updated: 11/13/2024

1 PRIVACY POINT OF CONTACT

Name	Lisa Hozey
Title	Information System Security and Privacy Officer (ISSPO)
Phone	202.229.5607
Email	hozey.lisa@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)*
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, please include if this is an existing system (either an annual recertification update or a major change).

***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. 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.

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.

No privacy controls are inherited from any external providers.

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. The sections of this MOA pertaining to privacy are summarized below:

Data Description

Data traversing between the Agency and the CISA CDM SSP 2.0 will include both Agency and CISA CDM unclassified operational and administrative data and will traverse existing internet connections using Hypertext Transfer Protocol Secure (HTTPS).

Data Sensitivity

The highest level of data that will be exchanged or processed between the Agency and the CISA CDM SSP 2.0 is Controlled Unclassified Information (CUI)Controlled Unclassified Information (CUI). Future requirements necessary to support the CDM capability of Identity and Access Management data collection services may include, but is not limited to, the following additional categories of data: Personally Identifiable Information (PII)), CUI, and Law Enforcement Sensitive data.

Services Offered

The data collected by the tools and sensors within this shared service environment is provided to the agency through the shared services integrator. The collected information is used and accessible by the agencies and CISA through the tools deployed within the CISA CDM SSP 2.0 which hosts the CDM Agency Dashboard.

Formal Security Policy

Policy documents that govern the protection of the data between the two organizations systems are DHS 4300A rev 13.1, July 27, 2017, and the Agency's latest released version of organizational security policies and regulations.

5. 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, 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**
  - *Physical Access Authorizations*
  - *Physical Access Control*
  - *Access Control for Transmission Medium*

- *Access Control for Output Devices*
- *Monitoring Physical Access*
- *Visitor Access Control*
- *Power Equipment and Cabling*
- *Emergency Shutoff*
- *Emergency Power*
- *Emergency Lightening*
- *Fire Protection*
- *Temperature and Humidity Controls*
- *Water Damage Protection*
- *Delivery and Removal*
- *Alternate Work Site*
- *Location of Information System Components*

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

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

  - *Password protection*
  - *Firewalls*
  - *Unique user identification names*
  - *Encryption*
  - *Intrusion Detection and Prevention Systems (IDPS)*
  - *Public Key Infrastructure (PKI) Certificates*
  - *Remote Access*
  - *Wireless Access*
  - *Audit events*
  - *Audit Storage capacity*
  - *Time Stamps*
  - *Authentication Management*
  - *Identification and Authentication/Identifier Management*
  - *Cryptographic key establishment and Management*

***Technical Controls are provided by PBGC, the CSP, and CISA*

- *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*

****Administrative Controls are provided by both PBGC and CISA*

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 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.

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.

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.

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?

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

2.3 Privacy Office Review

Name of Reviewer	Duane A. Dodson
Date Reviewed	11/06/2024
Expiration Date	11/06/2025
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

Enter description here.
