Pension Benefit
Guaranty Corporation

Information Technology Infrastructure Operations Department (ITIOD)

Zscaler Secure Access Service Edge (SASE) (PIA)

Last Updated: 08/14/2025

1 PRIVACY POINT OF CONTACT

Name	Lisa Hozey
Title	Information System Security and Privacy Officer (ISSPO)
Phone	202.487.8102
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.

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 13)*
SaaS: Zscaler Internet Access (ZIA) - Government (Secure Web Gateway - VTIC)	Designed to securely connect PBGC employees to externally managed applications, including SaaS applications and internet destinations regardless of device, location, or network, removing the need for traditional on-premises Virtual Private Network (VPN) appliances. ZIA provides a secure operating environment that meets the requirements of various compliance frameworks including the FedRAMP Moderate baseline. Solution includes broad functionality, which includes the following core services: • Access Control • Threat Prevention • Data Protection	No	N/A	N/A	N/A
SaaS: Zscaler Private Access (ZPA) -	A cloud-based security platform designed to provide	No	N/A	N/A	N/A

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 13)*
Government (Zero Trust Exchange - VPN Replacement)	access to and protect private enterprise applications by establishing a micro-tunnel between end users and devices to privately hosted applications (in PBGC data centers and Azure Virtual Data Centers (VDC's)).				
Software: **Zscaler Application (App) Connector**	The Zscaler App Connector is the front-end internal application that provides an authenticated secure interface between an internal app and the Zscaler cloud.	No	N/A	N/A	N/A
Zscaler Client Connector (ZCC)	The Zscaler Client Connector (ZCC) is the software installed on PBGC's endpoint devices that authenticates the endpoint with the ZPA cloud and forwards PBGC traffic to the Zscaler cloud from that endpoint.	No	N/A	N/A	N/A

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 13)*
Zscaler DLP Index Server	The DLP Index Server allows the configuration of index templates that can be applied when creating custom Data Loss Prevention (DLP) dictionaries and engines for the Zscaler Internet service (ZIA). The templates can be used for Exact Data Match (EDM) and Indexed Document Match (IDM).	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; 5 C.F.R. 731; 5 C.F.R. 302; OMB Circular A-130	N/A
Zscaler DLP Incident Receiver	The Zscaler Incident Receiver is a tool that allows PBGC to receive information about DLP policy violations securely, and to isolate policy-violating content for further inspection.	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; 5 C.F.R. 731; 5 C.F.R. 302; OMB Circular A-130	Yes
Zscaler Nanolog Streaming Server (NSS)	Zscaler Nanolog Streaming Service (NSS) allows streaming of all logs from the Zscaler Nanolog to PBGC's Security Information and Events Management (SIEM) system.	No	NA	NA	NA

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 13)*
Zscaler Log Streaming Server (LSS)	The Zscaler log streaming service provides log information about App Connectors and Users while accessing private applications. It allows streaming of all logs from LSS to PBGC's Security Information and Events Management (SIEM) system.	No	NA	NA	NA
Zscaler Digital Experience (ZDX)	The Zscaler Digital Experience (ZDX) service is built as a multi-tenant, cloud-based monitoring platform to probe, benchmark, and measure the digital experiences for every single PBGC user. ZDX proactively monitors every user device in PBGC to detect user experience and productivity issues.	No	NA	NA	NA

2.2 The System as a Whole

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

The Zscaler Secure Access Service Edge (SASE) cloud-solution integrates essential security functions including secure web gateways, firewall-as-a-service, cloud access security brokers, and data loss prevention (DLP). Zscaler SASE integrates with PBGC's existing centralized identity providers and device management software for device signaling and compliance checking to provide secure access to applications and data regardless of user, device, or device location in accordance with PBGC's risk tolerance.

Identity providers include Active Directory, Active Directory Federation Service (ADFS), and Entra ID. Integrated device management software include services such as CrowdStrike and Intune.

Zscaler SASE addresses Zero Trust requirements outlined in Executive Order (EO) M-22-09 to "to meet specific cybersecurity standards and objectives… to reinforce the Government's defenses against increasingly sophisticated and persistent threat campaigns."

The Zscaler SASE SaaS solution includes Zscaler Private Access (ZPA), Zscaler Internet Access (ZIA), and Zscaler Digital Experience (ZDX).

***ZPA** enables PBGC users to connect to private applications via App Connectors hosted in PBGC data centers and virtual data centers and no longer need to go through a termination appliance in the data center.*

***ZIA** securely connects PBGC employees to SaaS applications and the Internet regardless of device, location, or network, removing the need for traditional perimeter security tools, Trusted Internet Connections (TIC) based access, or VPN. ZIA includes broad functionality, with core services of Access Control, Threat Prevention, Data Protection, Advanced Threat Protection, and Cloud Sandbox.*

***ZDX** provides insight into device, network, and application performance to better understand user experience pain points with specific applications and services*

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.

There have been no changes since the last review.

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 ***Zscaler*** *component can be captured if the survey participants go to a site and sign a petition that is being sent to the Federal Government.*

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.

PII about employees, contractors are stored in PSIS. Genesis databases stores PII about participants and beneficiaries. PII is transmitted to the Zscaler Index Server to create a fingerprint for use in Exact Data Matching (EDM) policies. Additionally, Zscaler SASE uses regular expressions to identify patterns that match sensitive data types, such as SSNs. It also includes predefined templates for recognizing common data types, including PII. Exact Data Matching EDM enhances accuracy by matching exact data sets, reducing false positives, and ensuring that only precise matches trigger Data Loss Prevention (DLP) policies. Zscaler DLP Incident Receiver collects and forwards security incident data from Zscaler's security services, such as Zscaler Internet Access (ZIA) and Zscaler Private Access (ZPA), to a centralized logging point (Splunk) and Reportal. Splunk operates by collecting various types of security events and logs, normalizing and formatting the data to ensure compatibility with the destination system, and securely transmits it by using protocols like syslog or HTTPS. This process ensures that all security incidents are centralized, enabling efficient analysis, correlationand response by security teams.

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.

PII about employees, contractors are stored in PSIS. Genesis databases stores PII about participants and beneficiaries. PII is transmitted to the Zscaler Index Server to create a fingerprint for use in Exact Data Matching (EDM) policies.

Zscaler retrieves PII from Zscaler DLP policy violations that that has been set, unauthorized transmission of 1 exact data matching instance or 10 or more SSN number. Then these events are collected and sent to the Zscaler Incident receiver so that the security analyst can investigate the DLP incident.

When the DLP policy triggers, events are forwarded to the Zscaler Incident Receiver, which exclusively handles PII within the Zscaler SASE system for Security Operations (SECOPS) investigation. Privacy Act Statements are the responsibility of the business office (i.e., Office of Benefits Administration (OBA), Office of Management and Administration (OMA), Office of Information Technology (OIT), etc.) that directly collect PII from individuals and provide notice at the time of collection while providing opt-out options.

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

Zscaler processes approximately 3-5 million of records on individuals in the Zsclaer DLP tool - all PBGC employees and contractors, as well as pensioners and beneficiaries from Spectrum.

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.

PII about employees, contractors are stored in PSIS. Genesis databases stores PII about participants and beneficiaries. PII is transmitted to the Zscaler Index Server to create a fingerprint for use in Exact Data Matching (EDM) policies.

Zscaler does not require individuals to submit their PII. Zscaler retrieves PII from Zscaler DLP policy violations that that has been set, unauthorized transmission of 1 exact data matching instance or 10 or more SSN number. Then these events are collected and sent to the Zscaler Incident receiver so that the security analyst can investigate the DLP incident.

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?

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; 5 C.F.R. 731; 5 C.F.R. 302; OMB Circular A-130

While Zscaler does not collect SSNs directly from individuals, it does use SSNs collected by business units to restrict the unauthorized extractions from, or other unauthorized use of PII within, the PBGC network

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

*If **masking or tokenization** is enabled in the **Zscaler DLP Incident Receiver**, then in most cases it will **not contain full PII or sensitive data** — but it may still contain **derived sensitive metadata** that can be considered regulated depending on the compliance framework.*
Need to confirm with the SME if masking or tokenization is enabled.

Zscaler has a compelling business need to use SSNs as a primary identifier for the purposes outlined in section (a).

   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.

As PBGC is required to use SSNs as the primary identifier in several business units that collect SSNs directly from individuals and it is the most accurate way to prevent the unauthorized use or exfiltration of PII, there is no plan to reduce the use of SSNs as a primary identifier in Zscaler.

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.

The Zscaler DLP Incident Receiver is a backend component of Zscaler’s Data Loss Prevention (DLP) service that processes and manages alerts when policy violations are detected. Here’s how it works in practice.
When a user sends data through the Zscaler cloud (e.g., uploading a file, sending an email, posting form data), the traffic passes through Zscaler Enforcement Nodes (ZENs).

The ZENs apply the configured DLP policies — looking for sensitive data patterns (PII, PHI, PCI, custom regex, dictionaries, or structured/unstructured data).

If a match occurs, an incident is generated.

That incident is then sent to the DLP Incident Receiver, which is the centralized service responsible for collecting, normalizing, and storing these alerts.
The source systems are responsible for providing a privacy act statement to individuals

When the DLP policy triggers, events are forwarded to the Zscaler Incident Receiver, which exclusively handles PII within the Zscaler SASE system for Security Operations (SECOPS) investigation. Privacy Act Statements are the responsibility of the business office (i.e., Office of Benefits Administration (OBA), Office of Management and Administration (OMA), Office of Information Technology (OIT), etc.) which directly collects PII from individuals and provide notice at the time of collection while providing opt-out options.

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.

An Interconnection Security Agreement (ISA) has been initiated between Cybersecurity and Infrastructure Security Agency (CISA) Cloud Log Aggregation Warehouse (CLAW) and PBGC's Zscaler SASE, Azure Government (Azure-G), and Splunk. The purpose of this ISA is to document and seek the authorizing official's approval of a connection between CISA CLAW and PBGC's Zscaler SASE, Azure-G, and Splunk. This interconnection allows the transfer of PBGC metadata and log data to CISA. This ISA establishes individual and organizational security responsibilities for the protection and handling of unclassified information between CISA and PBGC. Additionally, this ISA documents the information to be transferred between CISA and PBGC.

14. For the user roles in the system:

Role Name	Number of Users in that Role	Approver	Access Level (Read, Write, etc.)	Recertification Date
Read Only Administrators	60	ITIOD System Owner	Read	May 2025
Full Administrators	4	ITIOD System Owner	Read/Write	May 2025
Users	2600	ITIOD System Owner	Read/Write	N/A, based upon GetITAccess requests and approvals

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*

- o *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.

A two-day training session through Zscaler Academy was completed in advance of the system's operational launch.

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).

- ***General Technology Management Records: GRS 3.1;Item 020***
    - *Retention and Destruction of PII: Destroy 3 years after agreement, control measures, procedures, project, activity, or transaction is obsolete, completed, terminated or superseded, but longer retention is authorized if required for business use.*
- ***Information Technology and Oversight Compliance Records GRS 3.1; Item 040***
    - *Destroy 5 years after the project/activity/transaction is completed or superseded, but longer retention is authorized if required for business use.*

ITIOD Retention Policy:

Audit Logs: The Zscaler system does not retain records beyond audit logs, which are forwarded to Splunk for retention and disposal.

2.3 Privacy Office Review

Name of Reviewer	Margaret Drake
Date Reviewed	8/19/2025
Expiration Date	8/19/2026
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
