Pension Benefit Guaranty Corporation

Information Technology Infrastructure Operations Department (ITIOD)

Zscaler Secure Access Service Edge (SASE) Privacy Impact Assessment (PIA)

Last Updated: 8/9/2024

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)*
Software as a Service (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) - Government (Zero Trust Exchange - VPN Replacement)	A cloud-based security platform designed to provide 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).	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 9)*
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
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	Yes
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	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;	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)*
	policy-violating content for further inspection.			5 C.F.R. 302; OMB Circular A-130	
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
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), part of ZIA, 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, please include if this is an existing system (either an annual recertification update or a major change).

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**, part of the ZIA component, 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. 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.

Zscaler indirectly sources PII due to its role in providing Data Loss Protection (DLP):

Zscaler does not collect PII from anyone or any system; rather, it receives encrypted data from PBGC users for downstream transport, decrypting this communication to provide DLP functions.

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. The business office (i.e., Office of Benefits Administration (OBA), Office of Management and Administration (OMA), Office of Information Technology (OIT), etc.) is responsible for a Privacy Act Statement on the form/system that collects the PII directly from the subject individuals.

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.

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.

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
Read Only Administrators	40-50	ITIOD System Owner	Read	May 2024
Full Administrators	10	ITIOD System Owner	Read/Write	December 2023
Users	2600	ITIOD System Owner	Read/Write	N/A, based upon GetITAccess requests and approvals

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 Controls are provided by Cloud Service Provided (CSP) and include controls and control enhancements in the following families:

- *Physical Access Authorizations*
- *Physical Access Control*
- *Access Control for Transmission*
- *Access Control for Output Devices*
- *Monitoring Physical Access*
- *Visitor Access Records*
- *Power Equipment and Cabling*
- *Emergency Shutoff*
- *Emergency Power*
- *Emergency Lighting*
- *Fire Protection*
- *Environmental Controls*
- *Water Damage Protection*
- *Delivery and Removal*
- *Alternate Work Site*

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

- *Authenticator Management*
- *Boundary Protection*
- *Identifier Management*
- *Cryptographic Protection*
- *System Monitoring (including Intrusion Detection and Prevention)*
- *Remote Access*
- *Wireless Access*
- *Event Logging*
- *Audit Log Storage capacity*
- *Time Stamps*
- *Cryptographic key establishment and Management (including both pre-placed keys and Public Key Infrastructure certificates)*

**Technical Controls are provided by both PBGC and the Cloud Service Provider (CSP)Administrative Controls - All PBGC users are required to complete privacy training annually. Administrative controls employed to secure the PII in the system include:*

- *Control Assessments*
- *System Monitoring*
- *Literacy Training and Awareness*
- *Alternate Storage Site*
- *Protection of Information at Rest*
- *Role-Based Training*
- *Least Privilege Personnel Screening*

Privacy Controls – Privacy controls are implemented by the system and include the following:

- *Role-Based Training | Processing PII*
- *Content of Audit Records | Limit PII Elements*
- *Incident Response Training | Breach*
- *Rules of Behavior | Social Media and External Site/Application Usage Restrictions*
- *Specific Categories of PII | Social Security Numbers, First Amendment Information*
- *Privacy Impact Assessments*
- *Information Management and Retention | Minimize PII in Testing, Training and Research*

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.

PII about employees and 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. This process ensures that all security incidents are centralized, enabling efficient analysis, correlation, and response by security teams.

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.

Zscaler Internet Access (ZIA): *When user traffic is directed through ZIA, it is inspected in real-time to enforce security policies such as threat detection and data loss prevention. The traffic is forwarded to the nearest Zscaler data center via secure tunnels (Generic Routing Encapsulation (GRE) or Internet Protocol Security (IPSec)) or through the Zscaler Client Connector. All data traffic, including Secure Sockets layer (SSL)/Transport Layer Security (TLS) encrypted traffic, is decrypted, inspected, and then re-encrypted before being forwarded to its destination. This ensures that even encrypted traffic is subject to the same security policies without compromising data integrity.*

Zscaler Private Access (ZPA): *ZPA provides secure remote access to internal applications without exposing them to the internet. It establishes microtunnels using TLS to connect users directly to applications based on user policies. These microtunnels are ephemeral and are*

established on a per-session basis, ensuring that data is encrypted end-to-end. This approach eliminates the need for traditional VPNs and reduces the attack surface by making applications invisible to unauthorized users.

Zscaler Application (App) Connector: *The Zscaler App connector is deployed within the same network as the other PBGC private applications it will secure. Users authenticate through the Zscaler Client Connector, which establishes a secure connection to the Zscaler cloud. This ensures that only authenticated users can access PBGC private applications. The App connector connects to the requested application within the private network, retrieves the necessary data, and sends it back through the Zscaler cloud to the PBGC user.*

Zscaler Client Connector (ZCC): *The ZCC client is installed on user devices to securely forward traffic to Zscaler services. It directs both internet-bound and internal application traffic to ZIA and ZPA respectively, using secure HTTPS connections. The client ensures that all user traffic is inspected, and policies are enforced regardless of the user's location, maintaining secure and compliant access to resources.*

Zscaler DLP Index Server: *The DLP Index Server scans PBGC data sources that have PII and creates fingerprints (templates)*

- *The hashes are sent to ZIA EDM DLP*
- *As traffic is inspected in ZIA DLP alerts may be triggered*
- *This detail (including violating content) is sent to the DLP Index Receiver and stored there*
- *If decided, this information could then be sent to Splunk*

Zscaler DLP Incident Receiver: *The DLP Incident Receiver collects and forwards security incident data from Zscaler services to centralized logging systems such as SIEMs and Reportal. This data flow involves the aggregation of security events and logs, which are normalized and securely transmitted using HTTPS to the destination systems. This ensures that incident data remains secure during transit and is readily available for further analysis and response.*

Zscaler Nanolog Streaming Server (NSS): *When an NSS receives the logs from the Nanolog, it decompresses and decodes them, applies the configured filters to exclude unwanted logs, converts the filtered logs to the configured output format so that they can be consumed and parsed by PBGC's SIEM.*

Zscaler Log Streaming Server (LSS): *LSS is deployed using two components: a log receiver and a ZPA App Connector. LSS resides in ZPA and initiates a log stream through a ZPA Public Service Edge. The App Connector resides in PBGC's enterprise environment. It receives the log stream and then forwards it to a log receiver.*

Zscaler Digital Experience (ZDX): *ZDX leverages Zscaler Client Connector and the Zscaler Zero Trust Exchange to actively monitor applications from an end user perspective. It continuously collects and analyzes various performance metrics, including application availability, response times, network hop-by-hop performance metrics, and device health*

metrics such as device configuration, Central Processing Unit (CPU), memory usage, process information, and device events.

By implementing these encrypted data flows and using protocols like HTTPS and TLS, Zscaler ensures that all data transmitted within its ecosystem is secure, maintaining the privacy and integrity of sensitive information across its services.

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.

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?

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?

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.

2.3 Privacy Office Review

Name of Reviewer	Ashley Church
Date Reviewed	8/9/2024
Expiration Date	8/9/2025
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.