Privacy Office Contact Information

Please send any questions by email to gsa.privacyact@gsa.gov or by U.S. Mail to:
General Services Administration
Chief Privacy Officer
1800 F Street NW
Washington, DC 20405

Document Purpose

This document contains important details about a GSA managed System, Application, or Project (identified below by the Authorization Package name). To accomplish its mission the GSA Office it supports must, in the course of business operations, collect personally identifiable information (PII) about the people who use such products and services. PII is any information [1] that can be used to distinguish or trace an individual's identity like a name, address, or place and date of birth.

GSA uses Privacy Impact Assessments (PIAs) to explain how it collects, maintains, disseminates, uses, secures, and destroys information in ways that protect privacy. This PIA comprises sections that reflect GSA's privacy policy and program goals. The sections also align to the Fair Information Practice Principles (FIPPs), a set of eight precepts codified in the Privacy Act of 1974.[2]

[1]OMB Memorandum Preparing for and Responding to the Breach of Personally Identifiable Information (OMB M-17-12) defines PII 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." The memorandum notes that "because there are many different types of information that can be used to distinguish or trace an individual's identity, the term PII is necessarily broad."

[2] Privacy Act of 1974, 5 U.S.C. § 552a, as amended.

General Information

PIA Identifier: 452
System Name: Security Tools (SecTools)
CPO Approval Date: 11/7/2024
PIA Expiration Date: 11/7/2027

Information System Security Manager (ISSM) Approval

Joseph Hoyt

System Owner/Program Manager Approval

Benjamin Peters

Chief Privacy Officer (CPO) Approval

Richard Speidel

PIA Overview

A: System, Application, or Project Name:
Security Tools (SecTools)

B: System, application, or project includes information about:

SecTools CORE consists of Operating Systems and Cloud Storage volume, AWS Services, and appliances that support SecTools Subsystems. Information coming into SecTools includes customer data that is decrypted, scanned, and re-transmitted as part of SecTool's Palo Alto border protection tools.

SecTools interfaces with multiple FISMA systems, and as such PII and other sensitive data in these FISMA system will pass through SecTools. PII datasets is written to the logs from any system holding PII or sensitive records that sends that information to ELP.

C: For the categories listed above, how many records are there for each?
SecTools interfaces with multiple FISMA systems, and as such PII and other sensitive data in these FISMA system will pass through SecTools. SecTools collects and processes a monthly aggregate of about 1.3 billion logs from IQ-FCS (a FISMA System) and 350 million logs from I-SecTools (a FISMA system).

D: System, application, or project includes these data elements:

- ENT passwords
- Individual Name/Contact Information
- Personal Email Addresses

Overview:

GSA IT SecTools is a diverse number of systems hosted in GSA's On Prem Data Center, in the AWS East and West Regions, and by SaaS Service Providers. Stennis is the primary On Prem Data Center, with RTP used as needed. Amazon US East and West are multi-tenant public clouds for Federal, State and Local Government customers, as well as commercial customers.
The Cloud Service Provider (CSP) for the SecTools environment is Amazon Web Services (AWS) East/West, which was granted a Provisional ATO (P-ATO) by FedRAMP Joint Authorization Board (JAB) in November 2017.
GSA IT SecTools is managed by the GSA Security Operations (SecOps) team and will be referred to as SecOps from this point forward. SecTools CORE consists of Operating Systems and Cloud Storage volume, AWS Services, and appliances that support SecTools Subsystems. SecTools provides services to other FISMA Federal Systems across GSA; those groups will be known as GSA SecTools Customers from this point forward.
Systems Receiving Controls from SecTools
The SecTools boundary consists of SecTools CORE and 10 subsystems:

1. DevSecOps - Applications that support DevSecOps operations for customers or SecTools.
2. Security Operation Center (SOC) as a Service (SOCaaS) - Security Information and Event Management (SIEM) applications, also known as the Enterprise Logging Platform (ELP).
3. Security Assessment - Vulnerability management tools.
4. Network Security - Networking applications, including Firewall, Intrusion Detection Systems/Intrusion Prevention Systems (IDS/IPS), and Microsegment solutions.
5. Governance Risk and Compliance (GRC) - Enterprise governance, risk, and compliance (GRC) applications across IT, finance, operations, and legal domains.
   Archer
6. Endpoint Agent Solutions - Endpoint Detection and Response (EDR) and Endpoint Protection Solutions used across the enterprise environment.
7. Identity, Credential, and Access Management (ICAM) - Identity management tools that support GSA GoCo Systems or CoCo Systems.
   CyberArk
8. Continuous Diagnostics and Mitigation (CDM) - Tools that deliver cybersecurity functions, integration services, and dashboards that help participating agencies improve their security posture.
9. Leveraged SaaS - Anything as a Service (XaaS) packages that support GSA Enterprise or other SecTools areas. They are FedRAMP Solutions that contain their own CRM requirements outside of the Subsystems Customer Responsibility Controls (CRM).
10. Firewall as a Service (FWaaS) - consists of tools that provide firewall filtering, internal and external traffic monitoring, intrusion detection and prevention, malware detection, content filtering and cloud perimeter protection.

1.0 Purpose of Collection

1.1: What legal authority and/or agreements allow GSA to collect, maintain, use, or disseminate the information?

5 U.S.C. 301; 40 U.S.C. 11315; 44 U.S.C. 3506; E.O. 9397, as amended; 5 U.S.C. 1001-14; 40 U.S.C. 3306.

1.2: Is the information searchable by a personal identifier, for example a name or Social Security number?
Yes

1.2a: If so, what Privacy Act System of Records Notice(s) (SORN(s) applies to the information being collected?
Existing SORN applicable

1.2: System of Records Notice(s) (Legacy Text): What System of Records Notice(s) apply/applies to the information?
SORN GSA/Agency-1

1.2b: Explain why a SORN is not required.

1.3: Has an information collection request (ICR) been submitted to or approved by the Office of Management and Budget (OMB)?

1.3: Information Collection Request: Provide the relevant names, OMB control numbers, and expiration dates.

1.4: What is the records retention schedule for the information systems(s)? Explain how long and for what reason the information is kept.
ELP active searchable logs are stored for 365 days. ELP cold storage records are stored for 913 days.

2.0 Openness and Transparency

2.1: Will individuals be given notice before the collection, maintenance, use or dissemination and/or sharing of personal information about them? No

2.1 Explain: If not, please explain.
SecTools does not have direct interface with individuals. SecTools interfaces with multiple FISMA systems, and as such PII and other sensitive data in these FISMA system will pass through SecTools. PII datasets is written to the logs from any system holding PII or sensitive records that sends that information to ELP.

3.0 Data Minimization

3.1: Why is the collection and use of the PII necessary to the project or system?
SecTools interfaces with multiple FISMA systems, and as such PII and other sensitive data in these FISMA system will pass through SecTools. PII datasets is written to the logs from any system holding PII or sensitive records that sends that information to ELP.

3.2: Will the system, application, or project create or aggregate new data about the individual?
No

3.2 Explained: If so, how will this data be maintained and used?

3.3 What protections exist to protect the consolidated data and prevent unauthorized access?
SecTools has implemented the required security and privacy controls according to NIST SP 800-53. The systems employ a variety of security measures defined in the System Security Plan (SSP) designed to ensure that information is not inappropriately disclosed or released.
Additionally, If any member of the SecTools team identifies PII data residing in any of the tools the team member will inform their supervisor who will follow the GSA Incident Reporting process and provide notification to the GSA-IR team.

3.4 Will the system monitor the public, GSA employees, or contractors?
None

3.4 Explain: Please elaborate as needed.

SecTools does not monitor GSA employees and contractors. SecTools interfaces with multiple FISMA systems, and as such PII and other sensitive data in these FISMA system will pass through SecTools. PII datasets is written to the logs from any system holding PII or sensitive records that sends that information to ELP.

3.5 What kinds of report(s) can be produced on individuals?
SecTools does not produce reports of individuals. However, If any member of the SecTools team identifies PII data residing in any of the tools the team member will inform their supervisor who will follow the GSA Incident Reporting process and provide notification to the GSA-IR team.

3.6 Will the data included in any report(s) be de-identified?
No

3.6 Explain: If so, what process(es) will be used to aggregate or de-identify the data?

3.6 Why Not: Why will the data not be de-identified?
SecTools does not produce reports of individuals. However, If any member of the SecTools team identifies PII data residing in any of the tools the team member will inform their supervisor who will follow the GSA Incident Reporting process and provide notification to the GSA-IR team.

4.0 Limits on Using and Sharing Information

4.1: Is the information in the system, application, or project limited to only the information that is needed to carry out the purpose of the collection?
Yes

4.2: Will GSA share any of the information with other individuals, federal and/or state agencies, or private-sector organizations?
None

4.2How: If so, how will GSA share the information?
N/A

4.3: Is the information collected:
From Another Source

4.3Other Source: What is the other source(s)?
Application logs

4.4: Will the system, application, or project interact with other systems, applications, or projects, either within or outside of GSA?
No

4.4WhoHow: If so, who and how?

4.4Formal Agreement: Is a formal agreement(s) in place?
No

4.4NoAgreement: Why is there not a formal agreement in place?
SecTools does not have any Memorandum of Understanding (MOU) or Interconnection Security Agreement (ISA) in place because the inflow of PII only occurs through logs.
SecTools interfaces with multiple FISMA systems, and as such PII and other sensitive data in these FISMA system will pass through SecTools. PII datasets is written to the logs from any system holding PII or sensitive records that sends that information to ELP.

5.0 Data Quality and Integrity

5.1: How will the information collected, maintained, used, or disseminated be verified for accuracy and completeness?
The PII information is only collected via customer data that is decrypted, scanned, and re-transmitted in application logs. Any member of the SecTools team that identifies PII data residing in any of the tools will inform their supervisor who will follow the GSA Incident Reporting process and provide notification to the GSA-IR team.

6.0 Security

6.1a: Who or what will have access to the data in the system, application, or project?
SecTools SecOps team

6.1b: What is the authorization process to gain access?
The SecTools SecOps team goes through a rigorous clearance process with background checks. Additional information about the access authorization is covered under the NIST SP 800-53 security and privacy controls defined in the SecTools CORE (and subsystems) System Security and Privacy Plan.

6.2: Has a System Security Plan (SSP) been completed for the Information System(s) supporting the project?
Yes

6.2a: Enter the actual or expected ATO date from the associated authorization package.
5/11/2023

6.3: How will the system or application be secured from a physical, technical, and managerial perspective?
SecTools has implemented the required security and privacy controls according to NIST SP 800-53. The systems employ a variety of security measures defined in the System Security Plan (SSP) designed to ensure that information is not inappropriately disclosed or released.

6.4: Are there mechanisms in place to identify and respond to suspected or confirmed security incidents and breaches of PII?
Yes

6.4What: What are they?
The system owner and Privacy Office rely on the GSA Information Breach Notification Policy to identify and address potential incidents and breaches. The Information System Security Officer (ISSO), Information System Security Manager (ISSM) along with other security personnel, coordinates the escalation, reporting and response procedures on behalf of the agency.

7.0 Individual Participation

7.1: What opportunities do individuals have to consent or decline to provide information?
SecTools does not have direct interface with individuals, but interfaces with multiple FISMA systems, and as such PII and other sensitive data in these FISMA system will pass through SecTools. PII datasets is written to the logs from any system holding PII or sensitive records that sends that information to ELP. As such, the option for individuals to consent/decline is not applicable.

7.1Opt: Can they opt-in or opt-out?
No

7.1Explain: If there are no opportunities to consent, decline, opt in, or opt out, please explain.
SecTools does not have direct interface with individuals, but interfaces with multiple FISMA systems, and as such PII and other sensitive data in these FISMA system will pass through SecTools. PII datasets is written to the logs from any system holding PII or sensitive records that sends that information to ELP. As such. As such, the option for individuals to consent/decline or opt in/opt out is not applicable.

7.2: What are the procedures that allow individuals to access their information?

SecTools does not have direct interface with individuals, but interfaces with multiple FISMA systems, and as such PII and other sensitive data in these FISMA system will pass through SecTools. PII datasets is written to the logs from any system holding PII or sensitive records that sends that information to ELP. As such, there is no requirement or opportunity for individual access requests.

7.3: Can individuals amend information about themselves?
No

7.3How: How do individuals amend information about themselves?

8.0 Awareness and Training

8.1: Describe what privacy training is provided to users, either generally or specifically relevant to the system, application, or project.
Security and privacy training is given through the OLU as part of the on-boarding process and annual refresher training to all GSA employees and contractors.

9.0 Accountability and Auditing

9.1: How does the system owner ensure that the information is used only according to the stated practices in this PIA?
System Owner ensures GSA employees and contractors take annual security and privacy training or their accounts will be deactivated.