Date of Approval: 05/09/2024
Questionnaire Number: 1189

Basic Information/Executive Summary

What is the name of your project (system, database, pilot, product, survey, social media site, etc.)?

GSS-34_CISCO_ISE-Unified_Access-Segmentation

Business Unit

IT - Cybersecurity

Preparer

For Official Use Only

Subject Matter Expert

For Official Use Only

Program Manager

For Official Use Only

Designated Executive Representative

For Official Use Only

Executive Sponsor

For Official Use Only

Executive Summary: Provide a clear and concise description of your project and how it will allow the IRS to achieve its mission.

Cisco Identity Services Engine (ISE) Unified Access-Network Segmentation (UA-SEG) is the IRS enterprise solution for network access controls. UA-SEG uses Cisco ISE installed on virtual-based appliances and is the identity and access control policy platform that enables enterprises to enforce compliance, enhance infrastructure security, and streamline their service operations. All authorized network devices and users must authenticate and be authorized on the IRS network to be allowed further access to the network or its information resources. If the credentials are not valid, the ISE - UA-SEG system rejects the connection attempt and reports it to the auditing controls in accordance with IRS policies, guidelines and standards.

Personally Identifiable Information (PII)

Will this project use, collect, receive, display, store, maintain, or disseminate any type of Sensitive but Unclassified (SBU), Personally Identifiable Information (PII), or Federal Tax Information (FTI)?

Yes

Please explain in detail how this project uses sensitive data from inception to destruction (data lifecycle).

Users of GSS-34 use the individually assigned SEID as part of the Identification and Authentication processes to access GSS-34 components.

Please select all types of Sensitive but Unclassified data (SBU)/Personally Identifiable Information (PII)/Federal Tax Information (FTI) that this project uses.

Internet Protocol Address (IP Address)
Standard Employee Identifier (SEID)

Cite the authority for collecting SBU/PII/FTI (including SSN if relevant).

PII for personnel administration - 5 USC

Product Information (Questions)

1.1 Is this PCLIA a result of the Inflation Reduction Act (IRA)?

No

1.3 What type of project is this (system, project, application, database, pilot/proof of concept, power platform/visualization tool)?

System

1.35 Is there a data dictionary for this system?

No

1.36 Explain in detail how PII and SBU data flow into, through and out of this system.

A user's name, machine/endpoint name is recognized by the Cisco ISE network by to the network identity (SEID and/or MAC address). The data is obtained from the workstation and validated via Active Directory or SmartID certificate. This information is then used to generate reports to resolve network access issues.

1.4 Is this a new system?

No

1.5 Is there a Privacy and Civil Liberties Impact Assessment (PCLIA) for this system?

Yes

1.6 What is the PCLIA number?

5424

1.7 What are the changes and why?

During FY24 FISMA Annual Security Control Assessment, it was determined that GSS-34 (UA-SEG) did not comply with Control RA-08, resulting in a Finding which states, “There are no PCLIAs documenting the system's SORN(s) and downstream audit logging system, Splunk”. Separate PCLIAs are required for all Systems and their Components.

1.8 If the system is on the As-Built-Architecture, what is the ABA ID of the system? If this PCLIA covers multiple applications shown on the ABA, please indicate the ABA ID for each application covered separated by a comma.

14.3.2

1.9 What OneSDLC State is the system in (Allocation, Readiness, Execution)?

Execution

1.95 If this system has a parent system, what is the PCLIA Number of the parent system?

PIA#7804 - MAIN - Intranet Routers, Switches and Load Balancers (IRSLB). Date of Approval: 05/09/2023 is the Parent system to PCLIA# 1189 (UA-SEG) & PCLIA# 1192 (Cisco-ISE).

2.1 If this system discloses any PII to any third party outside the IRS, does the system have a process in place to account for such disclosures in compliance with IRC 6103(p)(3)(A) or Subsection c of the Privacy Act? Contact Disclosure to determine if an accounting is required. Enter "Yes" or "No". If Exempt, type "Exempt".

No

2.2 Please provide the full name of and acronym of the governance board or Executive Steering Committee (ESC) this system reports to.

IT UNS Technology Infrastructures Board (TIB)

3.1 Does your project/system involve any use of artificial intelligence (AI), including virtual assistant, chat bot, and robotic process automation, as defined in Executive Order 13960?

No

3.3 Does this system use cloud computing?

No

3.31 Please identify the Cloud Service Provider (CSP), FedRAMP Package ID, and date of FedRAMP authorization.

This system does not use cloud computing.

3.6 Does this system interact with the public through a web interface?

No

3.7 Describe the business process allowing an individual to access or correct their information.

Due process is supported by user acceptance of the roles and responsibilities of the position, operator's manual and annual and routine user training for IT security role-based access. Annual IT security training requirements are enforced, system identification and verification processes employed; management supervision/direction over the staff performing system and/or business responsibilities is managed.

4.1 Who owns and operates the system (IRS Owned and Operated, IRS Owned and Contractor Operated, Contractor Owned and Operated)?

IRS Owned and Operated

4.2 If a contractor owns or operates the system, does the contractor use subcontractors?

No

4.5 Identify the roles and their access level to the PII data. For contractors, indicate whether their background investigation is complete or not.

(IRS Employees and Contractors) Only Role: System Administrator / Administrator Access (Contractors: Background Investigation Level: HIGH)

4.51 How many records in the system are attributable to IRS Employees? Enter “Under 50,000”, “50,000 to 100,000”, “More than 100,000” or “Not Applicable”.

Not Applicable

4.52 How many records in the system are attributable to contractors? Enter “Under 5,000”, “5,000 to 10,000”, “More than 10,000” or “Not Applicable”.

Not Applicable

4.53 How many records in the system are attributable to members of the public? Enter “Under 5,000”, “5,000 to 10,000”, “More than 10,000” or “Not applicable”.

Not Applicable

4.54 If records are attributable to a category not mentioned above in 4.51 through 4.53, please identify the category and the number of corresponding records to the nearest 10,000. If none, enter "Not Applicable".

Not Applicable

4.6 How is access to SBU/PII determined and by whom?

A potential user will request access via the (Online) BEARS system. This request must be approved by the potential user's manager based on a user's position and need-to-know.

5.11 Is there a Risk Assessment Form and Tool (RAFT) associated with this system on file with your organization or the IRS Risk Office.

No

5.2 Does this system use or plan to use SBU data in a non-production environment?

No

Interfaces

Interface Type

IRS Systems, file, or database

Agency Name

SPLUNK

Incoming/Outgoing

Both

Transfer Method

IPSEC TUNNEL

Systems of Records Notices (SORNs)

SORN Number & Name

IRS 34.037 - Audit Trail and Security Records

Describe the IRS use and relevance of this SORN.

Audit Trail and Security Records

SORN Number & Name

IRS 36.003 - General Personnel and Payroll Records

Describe the IRS use and relevance of this SORN.

General Purpose

Records Retention

What is the Record Schedule System?

General Record Schedule (GRS)

What is the retention series title?

IRS General Records Schedules (GRS) 3.2

What is the GRS/RCS Item Number?

020

What type of Records is this for?

Electronic

Please provide a brief description of the chosen GRS or RCS item.

All records housed in the Identity Services Engine (ISE) system will be erased or purged from the system in accordance with approved retention periods. It is not the official repository for data and documents and does not require National Archives approval to affect data disposition. Any new records generated by the system will be managed according to requirements under IRM 1.15.1 and 1.15.6 and will be destroyed using IRS General Records Schedules (GRS) 3.2, Item 020 for Access and Audit Logs, and as coordinated with the IRS Records and Information Management (RIM) Program and IRS Records Officer.

What is the disposition schedule?

Daily

Data Locations

What type of site is this?

System

What is the name of the System?

CISCO_ISE-Unified_Access-Segmentation

What is the sensitivity of the System?

Personally Identifiable Information (PII) including Linkable Data

What is the URL of the item, if applicable?

https://mtb012iseadm1.tier4.irs.gov

Please provide a brief description of the System.

Network Access Control and high value asset application protection.

What are the incoming connections to this System?

Incoming/outgoing connections: Network Devices (routers, switches, firewall) performing RADIUS authentication requests and receive response with ISE.

What are the outgoing connections from this System?

Incoming/outgoing connections: Network Devices (routers, switches, firewall) performing RADIUS authentication requests and receive response with ISE.