

Date of Approval: 04/05/2025
Questionnaire Number: 1809

Basic Information/Executive Summary

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

Venafi Control Plane

Acronym:

VCP

Business Unit

Information Technology

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.

Venafi Control Plane provides a holistic, and automated approach to enterprise certificate management lifecycle process. The tool will assist in providing human error factor from the lifecycle process. Venafi will automate renewal, installation, and validation on host systems. The organization is complete automation of certificate lifecycle management where possible that prevents human errors.

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).

Venafi Control Plane (VCP) scans the IRS IT systems to collect data relevant to the Certificate lifecycle management process for certificate automation. The survey is completed by the Public Key Infrastructure Project Management Office (PKI PMO) team for the certificate lifecycle management process as we will be using Sensitive but Unclassified (SBU) data. This is a new project being introduced into the IRS system, that we need to ensure that Venafi properly classified and noted in the PCLIA process. This is part of the 4.3 Initiative of IRA, to transform IRS IT systems and provide automation to the certificate management lifecycle process, that is only accessible to the PKI PMO team. The information includes Server Names, Server IP addresses, Secure Socket Layer (SSL) certificate data, owner groups, possible location data for the servers, associated group email address, SEIDs, and names. This system will utilize Active Directory for logon/Privilege User Management and Access Systems (PUMAS) application for credentials. Potential for non-admin access to the system would be granted using Business Entitlement Access Request (BEARS) administration/Single Sign-on (SSO) policies with SEID, Names, and employee email addresses. The benefit to the organization is complete automation of certificate lifecycle management where possible that prevents human errors.

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

SSN for personnel administration IRS employees - 5 USC and Executive Order 9397

Product Information (Questions)

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

Yes

1.2 What is the IRA Initiative Number?

IT Transformation & Modernization 4.3

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

Application

1.35 Is there a data dictionary for this system?

Yes

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

The application isn't public facing or have any taxpayer data. The information in the system is going to be considered employee SEID, name. The other information would be considered SBU, as it deals with the computer information found via scans, from Server name, IP address, certificate installed, where the certificate is installed (correctly or not correctly installed), data needed for issuance of new/renewed signed certificates, and if there are any self-signed certificates identify and email owner group to remediate the finding.

1.4 Is this a new system?

Yes

1.8 If the system is on the As-Built-Architecture (ABA), what is the ABA ID number of the system? If this PCLIA covers multiple applications shown on the ABA, please indicate the ABA ID number(s) for each application covered separated by a comma. If the system is not in the ABA, then contact the ABA (<https://ea.web.irs.gov/aba/index.html>) for assistance.

211591

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.

Enterprise Operations (EOPS)

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

3.6 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.

System will be integrated with Active Directory (AD), information provided will already be prepopulated with information from that system. Any changes will have to go through process already defined by AD, which is ticket with Human Relations (HR). The system doesn't have the ability to correct individual information, since it's feed from another source.

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

IRS Owned

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.

Public Key Infrastructure Project Management Office (PKI PMO) = System Administrator Developer Administrators-Admin rights to develop Managers-read Users-read/write

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

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

SBU/PII data (employee information) are on a need-to-know bases for the project. Data access will be determined as development progresses and Business Entitlement Access Request (BEARS) entitlements created. Specific access is

only granted to systems that are part of the certificate management lifecycle process.

5.1 Please describe any privacy risks, civil liberties and/or security risks identified for the system that need to be resolved and what is the mitigation plan?

None currently.

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?

Yes

5.3 Please upload the Approved Email and one of the following SBU Data Use Forms, Questionnaire (F14664) or Request(F14665) or the approved Recertification (F14659). Select Yes to indicate that you will upload the Approval email and one of the SBU Data Use forms.

Yes

Interfaces

Interface Type

IRS Systems, file, or database

Agency Name

Information Technology Servers

Incoming/Outgoing

Both

Transfer Method

Other

Other Transfer Method

Read only secure transport, all methods are encrypted

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.

Use AD directory user SEID information to allow access to the system. All employee interactions with the system are tracked and recorded.

Records Retention

What is the Record Schedule System?

Non-Record

What is the retention series title?

Venafi Records Retention

What is the GRS/RCS Item Number?

3.1

What type of Records is this for?

Electronic

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

There is SBU data in the application, there is no PII information so the application wouldn't be subject to the FOIA requests. However, data will be kept as necessary or issuance of certificate information. MS CA only encrypts the data the link is sent on; we do not keep the private key for SSL. We keep the public key stored on the HSM. Certificate Data even when expired/revoked always stays in the Microsoft CA database.

What is the Record Schedule System?

General Record Schedule (GRS)

What is the retention series title?

Information System Security Records GRS/RCS

What is the GRS/RCS Item Number?

3.2, Item 061

What type of Records is this for?

Electronic

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

Operation records relate to the certification application; certificate issuance and key generation (including key pair generation and private key loading and storage of private keys and components of private keys); certificate acceptance, validation, revocation, suspension, replacement, and renewal; creating and maintaining an event log; and installing and validating software updates.

What is the disposition schedule?

Disposition: Temporary. Destroy/delete when years 6 months to 20 years 6 months old, based on the maximum level of operation of the CA, or when no longer needed for business, whichever is later.