Date of Approval: 09/23/2024
Questionnaire Number: 1492

Basic Information/Executive Summary

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

DFNet

Business Unit

Criminal Investigation

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.

As financial investigators, IRS-Criminal Investigation (IRS-CI) fills a unique niche in the federal law enforcement community. Today’s sophisticated schemes to defraud the government and the American economy demand the analytical ability of financial investigators to wade through complex arrays of financial records. Records of transactions are moving from paper ledgers to computers to off-site, online storage. As a result, IRS-CI is developing tools and techniques to follow and find those records, wherever they may be. To perform digital evidence analysis, digital forensic examiners use high-powered forensic workstations that do not connect to the IRS network. These workstations, or endpoints, are made up of portable laptops, large storage solutions and desktop computing towers predominately utilizing the Windows operating system. Although effective, standalone workstations are limited in capability, decentralized and do not support cloud based forensic tools and security controls such as monitoring, patching and, auditing. The Digital Forensics Network (DFNet) aims to host forensic tools and create a single pane of glass infrastructure, thus improving forensic capability, workstation visibility and overall security posture. Digital Forensics employees are essential in collecting, storing, and presenting evidence collected in Federal court. Digital Forensics contains the expertise in computer and network forensics to address the need to forensically seize digital evidence. As the size and scope of digital evidence expands, IRS-CI must have the means and ability to expand our capabilities in real time. DFNet will afford IRS-CI the ability to remain agile in an ever-changing environment. DFNet is an off-network infrastructure solution that is physically and logically air-gapped from the IRS Enterprise Network. DFNet will utilize the implementation of the national internet contract for all of CIs field offices and posts of duty, which include all PODs where digital forensic examiners occupy. This internet contract and connectivity provide the infrastructure backbone that will allow DFNet to communicate between locations. DFNet is made up of Digital Forensics endpoints with access via Digital Forensic Lab network wired connection and encrypted remote access VPNs using mobile hotspots. Except for cloud-based license tracking and authentication, DFNet workstations have no direct connectivity to the internet. A centrally managed Virtual Desktop Solution (VDI) solution is provided for internet research and downloads. The primary purpose of DFNet is to deliver a secure standalone network for CI Digital Forensics functions, deploy cloud-based forensics licensing solutions, onboard forensic solutions requiring client-server architecture, and centralized management of security controls with a wide variety of Digital Forensic asset endpoints.

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).

Computer forensic examiners will participate in search warrants executed on residences and businesses and collect digital evidence from electronic devices in those residences and businesses that may contain PII. This system (DFNet) will host the forensic tools used by the forensic examiners to collect this digital evidence.

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

Address
Adoption Taxpayer Identification Number
Agency Sensitive Information
Alien Registration Number

Bar Codes
Biometric Information
Centralized Authorization File (CAF)
Citizenship or Migration Status
Comments (Social Media)
Credit Card Number
Criminal Investigation Information
Criminal Record
Document Locator Number (DLN)
Driver's License Number
Education Information
Email Address
Employer Identification Number
Employment Information
Family Members
Federal Tax Information (FTI)
Financial Account Number
Geographical Indicators
Global Intermediary Identification Number (GIIN)
Individual Taxpayer Identification Number (ITIN)
Internet Protocol Address (IP Address)
Language
Name
Non-Tax Proprietary data
Official Use Only (OUO) or Limited Office Use (LOU)
Online Identifiers
Other
Passport Number
Patient Number
Personal Characteristics
Photograph
Physical Security Information
Preparer Taxpayer Identification Number (PTIN)
Procurement Sensitive Data
Professional License Number
Protected Information
QR Codes
Social Security Number (including masked or last four digits)
Standard Employee Identifier (SEID)
Tax ID Number
Telephone Numbers
Universal Unique Identifier (UUID)
Vehicle Identification Number (VIN)

Please explain the other type(s) of PII that this project uses.

Anything that a person or business stores on their computers, phones, or other electronic devices could be interacted with on this system (DFNet).

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

Information by CI for certain money laundering cases - 18 USC
PII about individuals for Bank Secrecy Act compliance - 31 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)?

This project is a 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.

Computer forensic examiners collect data which may include PII during the execution of criminal search warrants and other criminal legal processes which is then temporarily stored on the DFNet laptops. After the search warrant is completed, the computer forensic examiners return to their computer labs and save the data off to external storage that is not part of this DFNet system and remove the data (including PII) from their DFNet laptops which thereby removes it from this DFNet system.

1.4 Is this a new system?

Yes

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

No not currently. This questionnaire is being completed to obtain a PCLIA for this system.

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.

This system is not on the As-Built-Architecture.

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

We are not following OneSDLC. We are in the readiness phase.

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

Parent system (Talon) does not have a PCLIA.

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".

Exempt

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

DFNet Steering Committee

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?

Yes. This system has virtual servers hosted in Microsoft Azure.

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

The CSP is Microsoft Azure; the Package D is F1603087869; the date is 1/3/24

3.32 Who has access to the CSP audit data (IRS or 3rd party)?

IRS

3.32 Does the CSP allow auditing?

Yes

3.33 Please indicate the background check level required for the CSP (None, Low, Moderate or High).

High

3.4 Is there a breach/incident plan on file?

Yes

3.5 Does the data physically reside in systems located in the United States and its territories and is all access and support of this system performed from within the United States and its territories?

Yes

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

This system does not interact with the public through a web interface.

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

We follow criminal legal processes as mandated by federal judges in search warrants and other similar legal orders. The federal criminal rules of evidence and legal processes have due process built into the process via the 4th and 5th amendments to the US Constitution.

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?

The system is IRS owned and operated.

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

There are forensic examiners and global system admins. There are NTFS permissions on the folders. There is a public folder for each user which the user has write permissions to and other users have read permissions. There is also a private folder for each user and only the user and their manager have access to that folder

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”.

All the data handled by this system is attributable to members of the public. The system, however, does not have a database so the data is not stored as records in a database. The data is in the form of files extracted from electronic devices owned by members of the public. These file extractions are legally authorized pursuant to a criminal search warrant issued by a federal judge. After the files are extracted, the data is not permanently stored within the system but is moved to offline storage for safekeeping for the duration of time that the criminal case is open and being adjudicated.

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

To get access to the DFNet system, users will be required to have the approved BEARS entitlement "LAN-CI-DFNET-LOCAL-ADMINS".

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?

No

Interfaces

Interface Type

Other Organization

Agency Name

the data is coming directly from people's homes and businesses

Incoming/Outgoing

Incoming (Receiving)

search warrant issued by federal court or other legal process

Transfer Method

Other

Other Transfer Method

the forensic examiners go to people's homes and businesses and physically copy the digital evidence

Systems of Records Notices (SORNs)

SORN Number & Name

No SORN

Please describe why a SORN is not needed.

Per IRM 10.5.6.3.3 (11-14-2023) (6) A file that temporarily has records for processing purposes that will be returned to a reported system upon completion is not subject to the SORN requirement if information in the temporary file can be located by reference to the reported file.

Records Retention

What is the Record Schedule System?

Non-Record

What type of Records is this for?

Electronic

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

Electronic evidence from search warrants.

What is the disposition schedule?

Our SOPs are to retain evidence one year past final adjudication of the case.

Data Locations

What type of site is this?

System

What is the name of the System?

DFNet

What is the sensitivity of the System?

Sensitive But Unclassified (SBU)

Please provide a brief description of the System.

Digital Forensics Network

What are the incoming connections to this System?

This is a closed system as described in the executive summary. Forensic examiners will use the system to extract data from electronic devices like cell phones and computers using their DFNet issued laptops.

What are the outgoing connections from this System?

The data extractions will then be copied to offline storage which is part of a separate system. There is no connection to this other system. The data transfer will be done using USB devices.