

Date of Approval: 06/22/2025
Questionnaire Number: 2356

Basic Information/Executive Summary

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

CMAP Employee Protection System (EPS)

Acronym:

Pega

Business Unit

Privacy, Governmental Liaison and Disclosure

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.

The Program Manager for the Office of Employee Protection (OEP) Pegasystems (Pega) Commercial-Off-the-Shelf (COTS) platform is the Chief, OEP, who reports to the Associate Director, Incident Management & Employee Protection under the Director, Privacy, Policy & Compliance in the Privacy Governmental Liaison & Disclosure Business Unit. There is one primary Pega Administrator and two back-up Pega Administrators. Pega is currently in a developmental migration process from the e-Trak EPS database. Pega is being developed in-house in 2025 using the e-Trak EPS database platform: EPS was converted from an Oracle database in 2009, and EPS migrated again to e-Trak in October 2019. If issues are encountered with Pega outside the scope of the Pega Administrators' capabilities, a Pega Administrator will email the Pega Team with a cc to their manager, Chief, Pega O&M Section. The purpose of Pega is to catalogue information and data

about Potentially Dangerous Taxpayer (PDT) and Caution Upon Contact (CAU) taxpayer cases. These cases identify taxpayers who represent a potential danger to the Internal Revenue Service (IRS) and IRS employees and/or contractors and include information as to why the taxpayer is considered a potential danger. Pega is a moderate risk application containing Sensitive but Unclassified (SBU) data and Personally Identifiable Information (PII), including information about the taxpayer, the nature of the incident, and the IRS employee (IRSE) or contractor who reported the incident. The PII that is collected includes, but is not limited to, the taxpayer's name, address, date of birth (DOB), Social Security Number (SSN), and Employer Identification Number (EIN), if applicable. The Pega database will receive information daily from the Treasury Inspector General for Tax Administration (TIGTA) via an Electronic File Transfer Utility. While the information in Pega is important to all IRS employees with public contact, the data is only accessible to authorized Office of Employee Protection (OEP) users who require access to perform their respective jobs and the Associate Director, PGLD IM&EP who signs off on all PDT/CAU cases that do not meet PDT or CAU criteria or where a nexus to tax could not be established for the taxpayer. In addition, if an IRSE who has a business "need to know" discovers a PDT or CAU indicator on a taxpayer's or Power of Attorney's (POA) IRS Integrated Data Retrieval System (IDRS) Master File/Non-Master File account(s) and that employee is unaware of why the taxpayer or POA is designated a PDT or CAU, the IRSE may enter the taxpayer's SSN or the POA's Centralized Authorization File (CAF) number in the EPS search box to obtain background information on the reason(s) for the PDT or CAU designation. In this instance, IRSE access is read-only. Limited access may also be granted to the Government Accounting Office or TIGTA for auditing purposes. In these instances, the access rights are temporary and read-only.

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).

Office of Management and Budget Circular A-130 requires federal agencies to develop a mitigation or elimination strategy for systems that use SSNs, which IRS continues to develop strategies to meet. An exception to this requirement is when the SSN is needed to uniquely identify a taxpayer (TP). SSNs are permissible under IRC 6109, which requires TPs to include SSNs on their income tax returns. The National Archives and Records Administration approved Pega EPS data disposition instructions on 5/3/07 under Job No. N1-58-07-2. EPS data is

approved for deletion/destruction after the Potentially Dangerous Taxpayer (PDT) or Caution upon Contact (CAU) indicator is removed. The BU maintains data stripped of personal identifiers in EPS archive for 5 years and then the record is permanently deleted from EPS archive after 5 years. EPS retention requirements (including inputs/outputs and system documentation) are published under Records Control Schedule 28 for Tax Administration-Collection, item 145. A) Inputs: Includes daily EPS referrals from TIGTA via EFTU and manual updates from investigative case files. Data includes TP identification, status information, and pertinent dates. AUTHORIZED DISPOSITION Delete/Destroy after input verification into EPS master files. B) Master Files: Maintains data relevant to TPs designated as PDT or CAU, including TIGTA investigation case file info and status reports of those TPs. AUTHORIZED DISPOSITION Delete/Destroy after PDT or CAU indicator is removed. Maintain data stripped of personal identifiers in EPS archive for 5 years and then the record is permanently deleted from EPS archive after 5 years. C) Outputs: Reports and ad-hoc queries pertaining to demographic info, number and types of designations, and other relevant trend and statistical data. AUTHORIZED DISPOSITION Delete/Destroy when superseded or no longer needed. D) System Documentation: Codebooks and user guide. AUTHORIZED DISPOSITION Delete/Destroy when superseded or obsolete.

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

- Address
- Biometric Information
- Centralized Authorization File (CAF)
- Citizenship or Migration Status
- Comments (Social Media)
- Criminal Investigation Information
- Criminal Record
- Email Address
- Employer Identification Number
- Employment Information
- Family Members
- Federal Tax Information (FTI)
- Individual Taxpayer Identification Number (ITIN)
- Internet Protocol Address (IP Address)
- Medical History/Information
- Name
- Online Identifiers
- Personal Characteristics
- Photograph
- Physical Security Information
- Preparer Taxpayer Identification Number (PTIN)
- Professional License Number
- Protected Information
- Social Security Number (including masked or last four digits)

Standard Employee Identifier (SEID)
Tax ID Number
Telephone Numbers

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

PII for federal tax administration - generally IRC Sections 6001 6011 or 6012
SSN for tax returns and return information - IRC section 6109

Product Information (Questions)

1 Is this PCLIA a result of a specific initiative or a process improvement?

No

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

System

3 What Tier designation has been applied to your system? (Number)

0

4 Is this a new system?

Yes

5 Is this system considered a child system/application to another (parent) system?

No

6 Indicate what OneSDLC State is the system in (Allocation, Readiness, Execution) or indicate if you go through Information Technology's (IT) Technical Insertion Process and what stage you have progressed to.

Readiness

7 Is this a change resulting from the OneSDLC process?

Yes

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

Privacy, Governmental Liaison & Disclosure (PGLD) Governance Board

9 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.

211650

10 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?

Yes

11 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 and 14110?

No

12 Does this system use cloud computing?

Yes

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

Pega Platform, F1306282198 (PCFG), 3/15/2019

12.2 Does the CSP allow auditing?

Yes

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

IRS

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

Moderate

13 Does this system/application interact with the public?

No

14 Describe the business process allowing an individual to access or correct their information. (Due Process)

The information within Pegasystems (Pega) COTS platform EPS comes from another IRS system, the Integrated Data Retrieval System (IDRS). This system provides the Privacy Act Notice to individuals. Pega does not directly provide individuals the opportunity to decline from providing information and/or from consenting to uses of the information. Notice, consent and due process are provided via IDRS and their related tax forms instructions, and pursuant to 5

USC. The IRS has the legal right to ask for information per IRC sections 6001, 6011, and 6012(a), and their regulations which state "taxpayers must file a return or statement with IRS for any tax they are liable for." Their response is mandatory under these sections.

15 Is this system owned and/or operated by a contractor?

No

16 Identify what role(s) the IRS and/or the contractor(s) performs; indicate what access level (to this system's PII data) each role is entitled to. (Include details about completion status and level of access of the contractor's background investigation was approved for.)

The EPS Specialist, EPS Management Assistant and EPS Inventory Management roles are all user roles with Read and Write access. The EPS Manager and EPS Associate Director roles are manager roles with Read and Write access. The EPS Administrator, Pega Developer and/or System Administrators are all administrator roles. Limited and temporary read-only access may also be granted to the Government Accounting Office (GAO) or TIGTA for auditing purposes. In addition, if an IRS employee (IRSE) who has a business need-to-know discovers a PDT or CAU indicator on a taxpayer's or Power of Attorney's (POA) IDRS Master File/Non-Master File account(s) and that employee is unaware of why the taxpayer or POA is designated a PDT or CAU, the IRSE may use the e-Trak EPS search feature and enter the taxpayer's SSN or the POA's CAF number to obtain background information on the reason(s) for the PDT or CAU designation. In this instance, IRSE access is read-only.

17 The Privacy Act of 1974 (5 USC § 552a(e)(3)) requires each agency that maintains a system of records, to inform each individual requested to supply information about himself or herself. Please provide the Privacy Act Statement presented by your system or indicate a Privacy Act Statement is not used and individuals are not given the opportunity to consent to the collection of their PII.

A Privacy Act Statement is not used, and individuals are not given the opportunity to consent to the collection of their PII as Pega EPS system does not collect information directly from taxpayers. The OEP receives information about taxpayers being considered for PDT and CAU consideration from third-party sources such as IRS employees, TIGTA, State Tax Agencies, IDRS, etc.

18 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".

Under 50,000

19 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".

Under 5,000

20 How many records in the system are attributable to members of the public? Enter "Under 100,000", "100,000 to 1,000,000", "More than 1,000,000" or "Not applicable".
Under 100,000

21 Identify any "other" records categories not attributable to the categories listed above; identify the category and the number of corresponding records, to the nearest 10,000; if no other categories exist, enter "Not Applicable".

Records attributable to TIGTA (TIGTA initiated referrals to OEP) - under 10,000;

Records attributable to State Tax Agency referrals to OEP - under 10,000.

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

The Chief, OEP determines who is granted access to SBU/PII information within Pega EPS. Only OEP employees and the PGLD IM&EP Associate Director who have authorized access to EPS are granted access to the data to perform their respective jobs. Limited access may be granted to the Government Accounting Office (GAO) or TIGTA for auditing purposes. In these instances, the access rights are temporary and read-only. A Business Entitlement Access Request (BEARS) is required for all users who need access to Pega EPS.

23 Is there a data dictionary on file for this system? Note: Selecting "Yes" indicates an upload to the Attachment Section is required.

No

24 Explain any privacy and civil liberties risks related to privacy controls.

The system does not maintain any information describing how any individual exercises their rights guaranteed by the First Amendment, nor is the system information used to conduct data mining as defined in the Implementing the Recommendations of the 9/11 Commission Act of 2007, Public Law 110-53, Section 804, and no computer matching occurs. The primary purpose is for the protection of IRS employees from potentially dangerous taxpayers and taxpayers who should be approached with caution. There is no plan to eliminate the use of SSNs in this system, since the entire purpose of the system is linked to the taxpayer's SSN. Without the SSN, there would be no ability to input the PDT/CAU indicators into Integrated Data Retrieval System (IDRS) or ensure that only warranted indicators are reflected on IDRS. The information within e-Trak EPS comes from another IRS program (IDRS). This system provides the Privacy Act Notice to individuals. The Pega EPS database does not directly provide individuals the opportunity to decline from providing information and/or from consenting to uses of the information. Notice, consent and due process are provided via IDRS and their related tax forms instructions, and pursuant to 5 USC. The IRS has the legal right to ask for information per IRC sections 6001, 6011, and 6012(a), and their regulations. The regulations state that "taxpayers must file a return or statement with IRS for any tax they are liable for." Their response is mandatory under these sections.

25 Please upload all privacy risk finding documents identified for the system (Audit trail, RAFT, POA&M, Breach Plan, etc.); click "yes" to confirm upload(s) are complete.

Yes

26 Describe this system's audit trail in detail. Provide supporting documents.

Case Management Applications Program (CMAP) EPS application has full audit trail capabilities. Amongst other things, the system records; logins, logouts, account creation, account deletions, timeouts, & locked accounts. The audit trail assures that those who use CMAP EPS only have permission to view and use the modules their role allows.

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

No

Interfaces

Interface Type

Other Federal Agencies

Agency Name

Treasury Inspector General for Tax Administration (TIGTA)

Incoming/Outgoing

Incoming (Receiving)

Transfer Method

Electronic File Transfer Utility (EFTU)

Interface Type

State Agencies

Agency Name

ALL 50 STATES

Incoming/Outgoing

Outgoing (Sending)

Transfer Method

Secure Data Transfer (SDT)

Systems of Records Notices (SORNs)

SORN Number & Name

IRS 60.000 - Employee Protection System Records

Describe the IRS use and relevance of this SORN.

Individuals attempting to interfere with the administration of internal revenue laws through assaults, threats, suicide threats,

filing or threats of filing frivolous criminal or civil legal actions against Internal Revenue Service (IRS) employees, or IRS contractors or the employees' or contractors' immediate family members, or through forcible interference against any officer, government contractor or employee while discharging the official duties at his/her position. An individual is designated as a Potentially Dangerous Taxpayer (PDT), based on verifiable information, furnished to the IRS Office of Employee Protection (OEP) or Treasury Inspector General for Tax Administration (TIGTA), that meets any of the OEP's established PDT criteria (1) through (5) or established OEP CAU criteria (1) through (3). An individual is designated as a taxpayer who should be approached with caution (CAU), based on reliable information furnished to the IRS OEP or the TIGTA, that meets any of the OEP's established CAU criteria (1) through (3).

SORN Number & Name

IRS 34.037 - Audit Trail and Security Records

Describe the IRS use and relevance of this SORN.

Records concerning the use of IRS computing equipment or other resources by employees, contractors, or other individuals to access IRS information; records concerning individuals whose information was accessed using IRS computing equipment/resources; records identifying what information accessed; records concerned the use of IRS computer equipment and other resources to send electronic communications; and records concerning the investigation of such incidents.

Records Retention

What is the Record Schedule System?

Record Control Schedule (RCS)

What is the retention series title?

Tax Administration - Collection

What is the GRS/RCS Item Number?

RCS 28, Item 145

What type of Records is this for?

Electronic

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

Employee Protection System (EPS). The EPS database (formerly the Potentially Dangerous Taxpayer System [PDTs]) identifies taxpayers who pose a threat to the safety of IRS employees whose official duties may require personal contact with such taxpayers.

What is the disposition schedule?

The National Archives and Records Administration (NARA) approved EPS data disposition instructions under Job No. N1-58-07-2, approved 5/3/2007. Data is approved for deletion/destruction after PDT or CAU indicator is removed from IDRS. The BU maintains data stripped of personal identifiers in EPS Archive for 5 years and then the record is permanently deleted from EPS archive after 5 years. EPS retention requirements (including inputs, outputs and system documentation) are published under Records Control Schedule (RCS) 28 for Tax Administration - Collection, item 145.

A. Inputs: Includes daily EPS referrals from TIGTA via file transfer protocol (FTP) scripts and manual updates from investigative case files. Data includes taxpayer identification, case summary, status information, and pertinent dates. AUTHORIZED DISPOSITION Delete/Destroy after input verification into EPS master files.

B. Master Files: Maintains data relevant to those taxpayers designated as either a Potentially Dangerous Taxpayer (PDT) or Caution Upon Contact taxpayer (CAU), including TIGTA investigation case file information, and reports regarding the status of those taxpayers. AUTHORIZED DISPOSITION Delete/Destroy after PDT or CAU indicator is removed. Maintain data stripped of personal identifiers in EPS Archive for 5 years and then the record is permanently deleted from EPS archive after 5 years.

C. Outputs: Reports and ad hoc queries pertaining to demographic information, number and types of designations, and other relevant trend and statistical data. AUTHORIZED DISPOSITION Delete/Destroy when superseded or no longer needed.

D. System Documentation: Codebooks and user guide. AUTHORIZED DISPOSITION Delete/Destroy when superseded or obsolete.

Data Locations

What type of site is this?

System

What is the name of the System?

Splunk

What is the sensitivity of the System?

Personally Identifiable Information (PII) including Linkable Data

Please provide a brief description of the System.

PCFG streams log data to the IRS Splunk environment via IRS EPZ, including Audit Logs, System Logs, and Monitoring Data. This ensures ongoing monitoring of platform performance and

security status. Provides ongoing monitoring of platform performance and security status.

What are the incoming connections to this System?

TCP for port forwarding of logs.