

Date of Approval: 10/15/2024
Questionnaire Number: 1523

Basic Information/Executive Summary

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

Box, Zixmail, XXXX

Acronym:

BZX

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.

BZX is the configuration and deployment of Box, ZixMail XXX XXXX on the Criminal Investigation (CI) network. Box is a cloud content management platform that facilitates secure collaboration and exchange of information between IRS CI and its internal and external partners. Box allows CI investigators and staff to conduct activities more efficiently and effectively, with greater visibility and security risk management in comparison to current state. ZixMail provides end-to-end email encryption to protect messages and attachments. ZixMail allows CI to encrypt emails and attachments sent to external partners. XXXX XX X
XXXXX XXXXXXXX XXXX XXXXXXXX XX XX XXXXXXXX XXXXXXXX
XXX XXXXXXXX XXX XXXXXXXX, XXXX XX XXXXXXXX XXXXXXXX
XXXX XXXX XXXXXXXX XXXXXXX. XXXXXXXXXXXXXXX, XXXXXXXX
XXXXXXXXXX XXXXXXXX XXXXXXXXXXXXXXX XXXXXXXX

XXXXXXXXXX XXXXXXXX XXX XXXXXXXX XX XX XXXXXXXX XX XXX
XXX XX XXXXXXXXXXXX XXXXXXXXXXXX.

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).

CI has implemented this secure external file transfer and collaboration service to enable CI to securely transfer case files and investigative data, too large to email, with external partners. These case files contain PII. CI Special Agents input PII data into their investigative documents. These documents then shared for case preparation with external partners e.g. DOJ. Only the recipient defined by Agents can open these documents with PII. All documents are purged from the Cloud system after 60 days. This ensures that no data is stored for a long time enabling potential breaches.

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)

Criminal Investigation Information

Criminal Record

Email Address

Employer Identification Number

Employment Information

Federal Tax Information (FTI)

Financial Account Number

Internet Protocol Address (IP Address)

Name

Passport Number

Photograph

Physical Security Information

Professional License Number

Social Security Number (including masked or last four digits)

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

PII for federal tax administration - generally IRC Sections 6001 6011 or 6012
PII for personnel administration - 5 USC
SSN for personnel administration IRS employees - 5 USC and Executive Order 9397
SSN for tax returns and return information - IRC section 6109

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)?

Project

1.35 Is there a data dictionary for this system?

No. The data is incapsulated in the Cloud database system, we are only being provided the service to it.

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

ZixMail and Box will primarily be used to share CI's investigative files with the US Attorney's Office and Department of Justice (DOJ) Tax. These files can include all types of PII information and vary dependent on the type of investigation. If working a Cybercrime case then IP information, SSN's, credit card numbers, etc. will most likely be sent. A general tax investigation will include copies of tax returns, SSN's, financial records, etc. With ZixMail this information will be sent encrypted to the recipient and if they are also a Zix customer, then it is saved in the recipient's email software. If they are not a Zix customer, then the email is accessible through a Portal /website and CI controls the length of time that the data will reside on the Portal. Box is similar in that CI controls the retention period for the data and it is planned to be stored temporarily and then removed after 60 days. XXXX XX X XXXXXXXX XXXX
XXXXXXXX/XXXXXXXX XXXXXXXX, XXX XXXXX XXX XXX XX
XXXX XXX XXXXXXXX XXX XXXXXXXXXXXXXXX XXXXXXXX, XXX
XXXX XX XXX XXXXXXXXXXXX XXX XXXXXX, XXXXXXXX XX
XXXXXXXX. XXXX XXXXXXXX X XXXXXXXX XXX XXXXXXXX
XXXXXXXX XX XXXX, XXX XXXXXX XX XXXXXXXX XXXX XXX XX
XXXXXXXXXX XXXX XX XXX XXX.

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?

6284

1.7 What are the changes and why?

No changes are made to BZX, PCLIA needs to be renewed.

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.

ABA ID for CI Box 211404 ABA ID for CI XXXX XXXXXX

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

Execution

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".

Yes

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

Criminal Investigation Governance Board, CI GB

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

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

XXXX XX XXXXXXXXXXXX, XX XXXX XXXXXXXXXXXXXXXX, XXXX

XX/XX/XXXX Box Enterprise Cloud Content Collaboration Platform, CI Box

F1212191840, Date 4/25/2016

3.32 Does the CSP allow auditing?

Yes

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

IRS has access to user activity logs.

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?

No

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

For Zixmail, access policy and process is inherited from GSS. ZixMail is available for all CI employees to use and is integrated into the Microsoft Outlook client. If a user is in Active Directory, they are authorized to use Zixmail. Access to Box XXX XXXX is requested via BEARS. Access is granted on a need-to-know basis. The Business Entitlement Access Request System (BEARS) enrollment process requires that an authorized manager approve access requests on a case-by-case basis. Access approval is based on the user's role(s) and responsibilities. Users are given the minimum set of privileges required to perform their regular and recurring work assignments. They are restricted from changing the boundaries of their access without management approval. The employee's access is terminated once they no longer require access to the application. Deletion from the active access role is also performed through BEARS.

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.

Users Read and write

Managers Read and write

System administrators Administrator

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”.

Under 50,000

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”.

More than 10,000

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

Access to Box XXX XXXX is requested via BEARS. Access is granted on a need-to-know basis. The Business Entitlement Access Request System (BEARS) enrollment process requires that an authorized manager approve access requests on a case-by-case basis. Access approval is based on the user's role(s) and responsibilities. Users are given the minimum set of privileges required to perform their regular and recurring work assignments. They are restricted from changing the boundaries of their access without management approval. The employee's access is terminated once they no longer require access to the application. Deletion from the active access role is also performed through BEARS. ZixMail is available for all CI employees to use and is integrated into the Microsoft Outlook client.

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?

There is no documented privacy risk.

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 Federal Agencies

Agency Name

DOJ, Treasury, other federal agencies

Incoming/Outgoing
Both
Transfer Method
Other
Other Transfer Method
Connecting to Cloud application

Interface Type

State Agencies
Agency Name
Various State and local agencies
Incoming/Outgoing
Both
Transfer Method
Other
Other Transfer Method
Connecting to Cloud application

Systems of Records Notices (SORNs)

SORN Number & Name

IRS 46.002 - Criminal Investigation Management Information
System and Case Files
Describe the IRS use and relevance of this SORN.
CI Information System

SORN Number & Name

IRS 34.037 - Audit Trail and Security Records
Describe the IRS use and relevance of this SORN.
Audit trail

Records Retention

What is the Record Schedule System?
General Record Schedule (GRS)
What is the retention series title?
GRS 5.2 Item 020 Intermediary records
What is the GRS/RCS Item Number?
GRS 5.2 Item 020
What type of Records is this for?
Electronic

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

Records that meet the following conditions:

- They exist for the sole purpose of creating a subsequent record and

- They are not required to meet legal or fiscal obligations, or to initiate, sustain, evaluate, or provide evidence of decision-making.

This includes certain analog and electronic source records for electronic systems that are not otherwise excluded. For specific examples, see the GRS 5.2 Frequently Asked Questions (FAQs). Exclusion: Source records that have been digitized. GRS 4.5, item 010, covers these records. Note: The GRS provides disposition authority for copies of electronic records from one system that are used as source records to another system, for example an extracted data set. The GRS does not apply to either the originating system or the final system in which the final records reside. These systems must be disposed of per an agency-specific schedule, or if appropriate, another GRS. It is possible that sometimes information is moved from one system to another without the creation of an intermediary copy. Temporary. Destroy upon creation or update of the final record, or when no longer needed for business use, whichever is later.

What is the disposition schedule?

Records purged after 60 days