

Date of Approval: **June 10, 2020**

PIA ID Number: **5078**

SYSTEM DESCRIPTION

Enter the full name and acronym for the system, project, application and/or database.

Box, ZixMail, BZ

Is this a new system?

Yes

What governance board or Executive Steering Committee (ESC) does this system report to? Full name and acronym.

Criminal Investigation Governance Board

Current ELC (Enterprise Life Cycle) Milestones:

System Development/Milestone 4B

Is this a Federal Information Security Management Act (FISMA) reportable system?

Yes

GENERAL BUSINESS PURPOSE

What is the general business purpose of this system? Provide a clear, concise description of the system, application or database, the reason for the system, and the benefits to the IRS to use the information, and how the information will be used.

BZ is the configuration and deployment of Box, ZixMail on the CI network. Box is a cloud content management platform that facilitates secure collaboration and exchange of information between IRS Criminal Investigation (CI) and its internal and external partners. Box would allow 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 will allow CI to encrypt emails and attachments sent to external partners.

PII DETAILS

Does the system use, collect, receive, display, store, maintain, or disseminate IR Code 6103 taxpayer information; or any other type of Sensitive but Unclassified (SBU) information or PII such as information about IRS employees or outside stakeholders?

Yes

Does the system use, collect, receive, display, store, maintain, or disseminate Social Security Numbers (SSN's) or tax identification numbers (i.e. last 4 digits, etc.)?

Yes

What types of tax identification numbers (TIN) apply to this system?

Social Security Number (SSN)

List the approved Treasury uses of the SSN:

Law enforcement and intelligence purposes

Explain why the authorized use(s) above support the new or continued use of SSNs (or tax identification numbers).

These systems will be used to share and research information in criminal investigations.

Describe the planned mitigation strategy and forecasted implementation date to mitigate or eliminate the use of SSN's (or tax identification numbers).

There is no plan to eliminate the use of SSN's. The SSN/EIN/TIN's are temporarily stored and automatically purged after 60 days. User activities will be logged to aid with incident response and to attribute events and user activities to unique identities.

Employer Identification Number

Other Taxpayer Identification Number

Does this system use, collect, receive, display, store, maintain or disseminate other (non-SSN) PII (i.e. names, addresses, etc.)?

Yes

Specify the PII Elements:

Name

Mailing address

Phone Numbers

E-mail Address

Date of Birth

Place of Birth

Mother's Maiden Name

Internet Protocol Address (IP Address)

Criminal History

Certificate or License Numbers

Vehicle Identifiers

Passport Number

Alien Number

Financial Account Numbers

Employment Information

Tax Account Information

Does this system use, collect, receive, display, store, maintain, or disseminate SBU information that is not PII?

Yes

Specify the types of SBU from the SBU Types List

Criminal Investigation Information Information concerning IRS criminal investigations or the agents conducting the investigations.

Are there other types of SBU/PII used in the system?

Yes

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

PII for federal tax administration is generally Internal Revenue Code Sections 6001, 6011, & 6012e(a)

SSN for tax returns and return information is Internal Revenue Code Section 6109

PII about individuals for Bank Secrecy Act compliance 31 USC

Information by CI for certain money laundering cases may be 18 USC

Has the authority been verified with the system owner?

Yes

BUSINESS NEEDS AND ACCURACY

Explain the detailed business needs and uses for the SBU/ PII, and how the SBU / PII is limited only to that which is relevant and necessary to meet the mission requirements of the system. If SSNs (or tax identification numbers) are used, explicitly explain why use of SSNs meets this criteria. Be specific.

These systems will be used to effectively preserve, collect, analyze, and disseminate criminal investigative data and required documentation in support of IRS Criminal Investigation's mission. These new applications provide users (Special Agents, analysts and professional staff) with the necessary infrastructure to securely access and collaborate on evidentiary case data, internet information and documents with external authorized partners. Criminal investigative case work requires evidentiary data and documents to be expeditiously and securely accessible to assigned personnel and law enforcement partners to effectively enforce United States' tax laws and other federal statutes. SSNs are required for cases that point to an individual and are unique to the individual.

How is the SBU/PII verified for accuracy, timeliness and completion?

Investigative purposes require that these data elements be collected to support the investigation regardless of whether or not another source exists.

PRIVACY ACT AND SYSTEM OF RECORDS

The Privacy Act requires Federal agencies that maintain a system of records to publish systems of records notices (SORNs) in the Federal Register for records from which information is retrieved by any personal identifier for an individual who is a US citizen or an alien lawfully admitted for permanent residence. The Privacy Act also provides for criminal penalties for intentional noncompliance.

Does your application or this PCLIA system pertain to a group of any record from which information is retrieved by any personal identifier for an individual who is a US citizen, or an alien lawfully admitted for permanent residence? An identifier may be a symbol, voiceprint, SEID, or other personal identifier that is used to retrieve information.

Yes

Identify the Privacy Act SORN(s) that cover these records.

IRS 34.037 Audit Trail and Security Records

IRS 46.002 Criminal Investigation Management Information System and Case Files

RESPONSIBLE PARTIES

Identify the individuals for the following system roles:

Official Use Only

INCOMING PII INTERFACES

Does the system receive SBU/PII from other systems or agencies?

Yes

Does the system receive SBU/PII from IRS files and databases?

No

Does the system receive SBU/PII from other federal agency or agencies?

Yes

For each federal interface, identify the organization that sends the SBU/PII, how the SBU/PII is transmitted and if there is an Inter-Agency Agreement (ISA) /Memorandum of Understanding (MOU).

Name: Department of Justice
Transmission Method: Box, ZixMail
ISA/MOU: No

Name: Department of Treasury
Transmission Method: Box, ZixMail
ISA/MOU: No

Name: Various other federal agencies
Transmission Method: Box, ZixMail
ISA/MOU: No

Does the system receive SBU/PII from State or local agency (-ies)?

Yes

For each state and local interface identify the organization that sends the SBU/PII, how the SBU/PII is transmitted and if there is an Inter-Agency Agreement (ISA) /Memorandum of Understanding (MOU).

Organization Name: Various State and local agencies
Transmission Method: Box, ZixMail
ISA/MOU No

Does the system receive SBU/PII from other sources?

Yes

Identify the source that sends the SBU/PII, how the SBU/PII is transmitted and if there is an Inter-Agency Agreement (ISA) /Memorandum of Understanding (MOU).

Organization Name: Financial Institutions
Transmission Method: Box, ZixMail
ISA/MOU No

Organization Name: Internet Service Providers
Transmission Method: Box, ZixMail
ISA/MOU No

Does the system receive SBU/PII from Taxpayer forms?

No

Does the system receive SBU/PII from Employee forms (e.g. the I-9)?

No

DISSEMINATION OF PII

Does this system disseminate SBU/PII?

Yes

Does this system disseminate SBU/PII to other IRS Systems?

No

Does this system disseminate SBU/PII to other Federal agencies?

Yes

Identify the full names of the federal agency(s) that receive SBU/PII from this system, and if there is an Inter-Agency Agreement (ISA) / Memorandum of Understanding (MOU).

Organization Name: Department of Justice
Transmission Method: Box, ZixMail
ISA/MOU No

Organization Name: Department of Treasury
Transmission Method: Box, ZixMail
ISA/MOU No

Identify the authority

Law Enforcement and Intelligence Purposes Exemption.

Identify the Routine Use in the applicable SORN (or Privacy Act exception)

Not a system of record. Law Enforcement and Intelligence Purposes Exemption.

For what purpose?

Law Enforcement and Intelligence Purposes Exemption.

Does this system disseminate SBU/PII to State and local agencies?

Yes

Identify the full names of the state and local agency(s) that receive SBU/PII from this system, and if there is an Inter-Agency Agreement (ISA) /Memorandum of Understanding (MOU).

Organization Name: Various State and Local Agencies
Transmission Method: Box, ZixMail
ISA/MOU No

Identify the authority

Law Enforcement and Intelligence Purposes Exemption.

Identify the Routine Use in the applicable SORN (or Privacy Act exception)

Not a system of record. Law Enforcement and Intelligence Purposes Exemption.

For what purpose?

Law Enforcement and Intelligence Purposes Exemption.

Does this system disseminate SBU/PII to IRS or Treasury contractors?

No

Does this system disseminate SBU/PII to other Sources?

Yes

Identify the other source(s) that receive SBU/PII from this system, and if there is an Inter-Agency Agreement (ISA) /Memorandum of Understanding (MOU).

Organization Name: Financial Institutions
Transmission Method: Box, ZixMail
ISA/MOU No

Organization Name: Internet Service Providers
Transmission Method: Box, ZixMail
ISA/MOU No

Identify the authority

Law Enforcement and Intelligence Purposes Exemption.

Identify the Routine Use in the applicable SORN (or Privacy Act exception)

Not a system of record. Law Enforcement and Intelligence Purposes Exemption.

For what purpose?

Law Enforcement and Intelligence Purposes Exemption.

PRIVACY SENSITIVE TECHNOLOGY

Does this system use social media channels?

No

Does this system use privacy-sensitive technologies such as mobile, global position system (GPS), biometrics, RFID, etc.?

No

Does the system use cloud computing?

Yes

Is the cloud service provider (CSP) Federal Risk and Authorization Management Program (FedRAMP) certified?

No

Please explain:

The BZ project consists of 1) Box - Box was FedRamp certified at the moderate level on March 24, 2017. 2) Zix - ZixMail is considered a managed service. ZixMail is a secure email service to send encrypted email to external partners. ZixMail security change request is in review by IT Cybersecurity who will provide applicable security assessment(s).

Please identify the ownership of the CSP data.

Third Party

Does the CSP allow auditing?

Yes

Who audits the CSP Data?

3rd Party

What is the background check level required for CSP?

High

Is there a breach/incident plan on file?

Yes

Privacy laws (including access and ownership) can differ in other countries. This cloud will be Continental US (CONUS) only for:

Storage

Transmission

Maintenance

Does this system/application interact with the public?

No

INDIVIDUAL NOTICE AND CONSENT

Was/is notice provided to the individual prior to collection of information?

No

Why not? If information is not collected directly from an individual, please discuss the factors considered in deciding to collect information from third party sources.

The components are designed and configured to be transitory in nature and not long-term storage solutions or repositories. The information being transferred may have originated through a summons, grand jury subpoena, search warrant or public records.

Do individuals have the opportunity to decline from providing information and/or from consenting to particular uses of the information?

No

Why not?

Information used for Criminal Investigation / Law Enforcement purposes.

How does the system or business process ensure 'due process' regarding information access, correction and redress?

Once a criminal case is referred for prosecution the individual will be permitted to rebut any of the information that was used to determine prosecution potential.

INFORMATION PROTECTION

Identify the owner and operator of the system (could be IRS owned and Operated; IRS owned, contractor operated; contractor owned and operated)

IRS Owned and Contractor Operated

The following people have access to the system with the specified rights:

IRS Employees

Users: Read Write

Managers: Read Write

System Administrators: Administrator

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

Access to Box will be requested via an Online (OL) Form 5081. Access is granted on a need-to-know basis. The OL5081 enrollment process requires that an authorized manager approve access requests on a case by case basis. Access approval is based on the Users 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 will be terminated once they no longer require access to the application. Deletion from the active access role is also performed through the OL5081. ZixMail will be available for all CI employees to use and is integrated into the Microsoft Outlook client.

RECORDS RETENTION SCHEDULE

Are these records covered under a General Records Schedule (GRS, IRS Document 12829), or has the National Archives and Records Administration (NARA) approved a Records Control Schedule (RCS, IRS Document 12990) for the retention and destruction of official agency records stored in this system?

No

You must work with the IRS Records and Information Management (RIM) Program Office to address records retention requirements before you dispose of any records in this system.

SA&A OR ASCA

Has the system been through SA&A (Security Assessment and Authorization) or ASCA (Annual Security Control Assessment)?

In-process

When is the anticipated date of the SA&A or ACS completion?

6/24/2020

Describe the system's audit trail.

CI users will be using their CI devices which are fully audited and logged at the FISMA High level using the existing GSS systems, policies and procedures. The three services will be logging events and forwarding them to CI managed event logging solutions, InTrust and/or Splunk. Security events will be reviewed by CI Cybersecurity staff using dashboards, automated reports/alerts, etc. Logs will be reviewed periodically by management to validate authorized usage. CI staff will follow CI Incident response plan to respond to any findings.

PRIVACY TESTING

Does the system require a System Test Plan?

Yes

Is the test plan completed?

Yes

Where are the test results stored (or documentation that validation has occurred confirming that requirements have been met)?

Testing is expected to begin in next few weeks and will be stored on CI BZ SharePoint site.

Were all the Privacy Requirements successfully tested?

Yes

Are there any residual system privacy, civil liberties, and/or security risks identified that need to be resolved?

No

Describe what testing and validation activities have been conducted or are in progress to verify and validate that the applicable Privacy Requirements (listed in header) have been met?

508 testing and UAT to be completed.

SBU DATA USE

Does this system use, or plan to use SBU Data in Testing?

No

NUMBER AND CATEGORY OF PII RECORDS

Identify the number of individual records in the system for each category:

IRS Employees: Under 50,000

Contractors: Not Applicable

Members of the Public: Under 100,000

Other: No

CIVIL LIBERTIES

Does the system maintain any information describing how any individual exercises their rights guaranteed by the First Amendment?

No

Is the system information used to conduct 'data-mining' as defined in the Implementing Recommendations of the 9/11 Commission Act of 2007, Public Law 110-53, Section 804?

No

Will this system have the capability to identify, locate, and monitor individuals or groups of people?

No

Does computer matching occur?

No

ACCOUNTING OF DISCLOSURES

Does the system include or require disclosure of tax or employee information to anyone other than IRS employees in the performance of their duties, or to the person to whom the information pertains or to a 3rd party pursuant to a Power of Attorney, tax or Privacy Act consent?

Yes

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.

Yes