Date of Approval: **August 18, 2021**

PIA ID Number: **6284**

SYSTEM DESCRIPTION

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

Box, ZixMail, XXXX XXXXXXXXXX, BZX

Is this a new system?

No

Is there a PCLIA for this system?

Yes

What is the full name, acronym, and milestone of the most recent PCLIA?

Box, Zixmail, XXXX, BZX

What is the approval date of the most recent PCLIA?

6/10/2020

Changes that occurred to require this update:

Significant System Management Changes

Were there other system changes not listed above?

No

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:

Operations & Maintenance (i.e., system is currently operational)

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.

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 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. XXXX XX X XXXXX XXXXXXX XXXXX XXXX XXXXX XX XX XXX XXXX XXXXXXXXXXXXXXXX XXXXXXXX XX XXXXXXX XXXXXXXX XXX XXXXXXX XXXX XXXXXXXXX XXXXXX XX XXXXXXX XXXXXXXXX XXXX XXXXX XXXXXXX XXXXXXXX XXXXXXXXXXXX, XXXXXXX XXXXXXXXX XXXX XXXXXXX XXXXXXXXXXXXX XXXXXXX XXXXXXXXX XXXXXXX XXX XXXXXX XX XX XXXXXXX XX XXX XXX XX XXXXXXXX XXXXXXXXXX

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
Standard Employee Identifier (SEID)
Mother's Maiden Name
Protection Personal Identification Numbers (IP PIN)
Internet Protocol Address (IP Address)
Criminal History
Medical Information
Certificate or License Numbers
Vehicle Identifiers
Passport Number
Alien Number
Financial Account Numbers
Photographic Identifiers
Biometric Identifiers
Employment Information
Tax Account Information
Centralized Authorization File (CAF)

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:

Agency Sensitive Information Information which if improperly used or disclosed could adversely affect the ability of the agency to accomplish its mission.

Official Use Only (OUO) or Limited Official Use (LOU) Information designated as OUO or LOU is information that: is exempt under one of the statutory Freedom of Information Act exemptions; is prohibited by other laws or regulations; would significantly impede the agency in carrying out a responsibility or function; or would constitute an unwarranted invasion of privacy.

Proprietary data Business information that does not belong to the IRS.

Protected Information Information which if modified, destroyed, or disclosed in an unauthorized manner could cause loss of life, loss of property or funds by unlawful means, violation of personal privacy or civil rights, gaining of an unfair procurement advantage by contractors bidding on government contracts, or disclosure of proprietary information entrusted to the Government.

Physical Security Information Security information containing details of serious weaknesses and vulnerabilities associated with specific systems and facilities.

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?

XXX

Describe the other types of SBU/PII that are applicable to this system.

XXXXXXX XXX XXX XXXX XXXXXXXXX XX XXXX XX XXXXX XXXX XXXXXXXXXXXXX XXXXX XXXX XXX XX XXXXXXXXXX XXXXXX XXX XXXXXXXXXX XX XXXXXXX XXXXX XXXX XXXXX XXXXX XXX XXXXXXX XXX XXXXX XX XXX XXXXXXXXXXX XXX XXXX XXXXXXXXX XX XXX XXXX XX XXXXXXXXXXXXXX XX XXXXXXX X XXXXXXXXXX XXXX XXXX XX XXXXXXXXXXXXX XXXXXX XXXXXX XXXX XXXXXXXX XXXX XXXX XXXX XXXXXXX XX XXXXX X XXXXXXX XXX XXXXXXXXXXXXX XXXX XXXXXXX XXXXXX XX XXX XXXXXXXX XXXXXX XXXXXXXXX XXXXXXXX XXXX XXXX XXXXXXX XXXX XXXXXXXXXXX XXXX XX XXXX XXXXXXXXX XX XXX XXXXXXXXX XXX XX XXXX XXX XXXX X XXX XXXXXXXXX XXXX

XX XX XXXXX XX XXX XXXXXXXXXXX XXXXX XXXXXXXXX XX XXXX XXX XXX X XXX XXXXXXXX XXXX XXX XXXXX XX XXXXXXXXXX XXXXXXX X XXXXXXXXXXXXXXX XXX XX XXXXXXXX XXX XXXXXXX XX XXXX XXXX XXX XXXX XXXX XXXXXX XX XXX XXXXXXX XXX XX XXXXXXX XX XXXX XX XXXXXXXX XXX XXXXXXXXX XXXXXX XXX XXX XXXX XXX XX XX XXXXXXX XX XX XXXXXX XXXXXXXXXXX XXX XXXX XXXXXXX XXXXX XX XXXX. XXXX XX X XXXXXXX XXXX XXXXXXXXXXXXXXXX XXXXXXXXX XXXX XXXXX XXX XX XXXX XXX XXXXXXXX XXX XXXXXXXXXXXXX XXXXXXXX XXX XXXX XX XXX XXXXXXXXXXX XXX XXXXXXX XXXXXXXX XX XXXXXXXX XXXXX XXXXXXXX X XXXXXXXX XXX XXXXXXXXX XXXXXXXX XX XXXXX XXX XXXXXX XX XXXXXXX XXXX XXX XX XXXXXXXXX XXXX XX XXX XXXX

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 Treasury
Transmission Method: Box, Zixmail
ISA/MOU: No

Organization Name: Department of Justice
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?

XXX XXXXXXXXXXX XXX XXXXXXXXXXXX XXXXXXXX XXXXXXXXXX XXXXXXX X XXXXXXX XX XXXXXXXXXXXX XXXXXXXXXXX XXXXXXX XXXXXXXX XXXX XX XXXXXXXXXX XX XXXXXXX XXX XXXXXXXXXX XX XXXXXXXXX

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?

XXX XXXXXXXXXXX XXX XXXXXXXXXXX XXXXXXXX XXXXXXXXXX XXXXXX X XXXXXXX XX XXXXXXXXXXX XXXXXXXXXXX XXXXXXX XXXXXXXXXX XXXX XX XXXXXXXXXX XXXXX XXX

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. XXX XXXXXXXXXXX XXX XXXXXXXXXXXX XXXXXXXX XXXXXXXXXX XXXXXXX X XX XXXXX XXXXXXXXXX XXX XXXXXXXXX XXXXXXXXXXXXX XXXXX XXXXXXX XXXXX XXXXXXX XXXXXXXXXX XXXXXXXXXXXX X XXXXXXXX XXXXXXX XXXXXXXXX XXX XXXXX XXXXXXXXX XXXX XXXXXXXX XXX XX XXXXXX XXXXXXXXXXXXXX

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 BZX project XXXXXXXX XX X XXXXXXXXXX: 1) Box - Box was FedRamp certified at the moderate level on March 24, 2017. They are currently in the certification process for FedRamp high, and they have implemented high-impact controls. 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). XXXXXXX XXX XXX XXXXXXXXX XXXXXXXX XXXXXXXXXXXXXX XX XXXXXX XXX XXX XXXX XXXX XXX XXXX XXX XXXXXXXX XXXX XXX XXX XXXXXX XX XXXX X XXXX XX XXXX XXX XXXXXXXXXXXXXXXX XXXXXXXX XXXXXXXXX XX XX XXX XXXX XX XXXXX XX XXXXXXXXXX XXXX XXXXXXXXX XX XXXXXXXXXXXXXX XXXXXXXXXX XXXX XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXXXXXXXX XX XXXXXXXXXX XXX XX XX XX XXX XXXXXXXX XX XXXXXXXX XXXX XXXX XXXX XXXXXXXXXX XX XXXXXX XXX XXXXXXXXXX XX XXX XXXX XXXXXXXXXX XXX XXXXX XXXX XXXXXXXX XXXXX XXXX XXXXXXX XXXX XX XX XX XXXXXXX XXX XXXXXXXX XXXXXXXXXXXXXX XX XXXXXXX XXXXX XXXX XXX XXX XXXXXXX XXXXXXXXXX XX XXXX XXXXX

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 XXX XXXX will be 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 will be terminated once they no longer require access to the application. Deletion from the active access role is also performed through BEARS. 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?

Yes

How long are the records required to be held under the corresponding GRS or RCS, and how are they disposed of? In your response, please provide the GRS or RCS chapter number, the specific item number, and records series title.

All records housed in the Box, ZixMail, XXXX XXXXXXXXXX will be erased or purged from the systems in accordance with approved retention periods. It is not the official

repository for data and documents and does not require National Archives approval to affect data disposition. Any new records generated by the system will be managed according to requirements under IRM 1.15.1 and 1.15.6 and will be destroyed using General Records Schedules (GRS) 3.2, Items 030, 031 and GRS 6.1, items 010, 011, 012 as coordinated with the IRS Records and Information Management (RIM) Program and IRS Records Officer.

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?

12/22/2021

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 XXXX XXX systems, policies, and procedures. The XXXXX services will be logging events and forwarding them to XXXX XXX managed event logging solution CI-1 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 plans 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 prior to the Event Driven Security Assessment (ESCA) and will be stored on the CI BZX 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?

Box and Zixmail have completed ESCA/Security testing and are maintained with System Security Plans (SSP), 508 (Information Technology handicap accessibility guidelines) testing and User Acceptance Testing (UAT) have been completed. XXXX XXX XXXXXXXX XXXX XXXXXXXXXX XXXXXXX XXX XXX X XXXX XX XXXXX XXX XXX XXX XXXXXXXX XXXXXXX XXXXX XX XXX XXXXXXXX XXX XXXX XXXXXXX XXX XXX XXXXXXXX XXXXXXX XXXXXXX XX XX XXXXXX XXX XXXX XXXXX XXXX XX XXX XXXXXXX XXXXXXXXX

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