Privacy and Civil Liberties Impact Assessment
for the

Treasury Government Security Operations Center Network

November 28, 2017

Reviewing Official
Timothy H. Skinner
Director, Privacy and Civil Liberties, Privacy, Transparency & Records
Department of the Treasury

Bureau Certifying Official
Ryan Law
Deputy Assistant Secretary for
Privacy, Transparency, and Records
Department of the Treasury

Section 1: Introduction

It is the policy of the Department of the Treasury ("Treasury" or "Department") and its Bureaus to conduct a Privacy and Civil Liberties Impact Assessment ("PCLIA") when personally identifiable information ("PII") is maintained in a system or by a project. PCLIAs are required for all systems and projects that collect, maintain, or disseminate PII, regardless of the manner in which the information is retrieved.

This assessment is being completed pursuant to Section 208 of the E-Government Act of 2002 ("E-Gov Act"), 44 U.S.C. § 3501, Office of the Management and Budget ("OMB") Memorandum 03-22, "OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002," and Treasury Directive 25-07, "Privacy and Civil Liberties Impact Assessment (PCLIA)," which requires Treasury Offices and Bureaus to conduct a PCLIA before:

1. developing or procuring information technology ("IT") systems or projects that collect, maintain or disseminate PII from or about members of the public, or

2. initiating a new collection of information that: a) will be collected, maintained, or disseminated using IT; and b) includes any PII permitting the physical or online contacting of a specific individual, if identical questions have been posed to, or identical reporting requirements imposed on, 10 or more persons. Agencies, instrumentalities, or employees of the federal government are not included.

This PCLIA provides the following information regarding the system or project:

(1) an overview of its purpose and functions;
(2) a description of the information collected;
(3) a description of the how information is maintained, used, and shared;
(4) an assessment of whether the system or project is in compliance with federal requirements that support information privacy; and
(5) an overview of the redress/complaint procedures available to individuals who may be affected by the use or sharing of information by the system or project.

The Treasury Government Security Operations Center Network has been in place for many years. A Privacy Threshold Assessment (PTA) and Privacy Impact Assessment (PIA) were completed in 2011. This PCLIA will replace the existing PTA/PIA.

Section 2: Definitions

Agency – means any entity that falls within the definition of the term "executive agency"' as defined in 31 U.S.C. § 102.

Certifying Official – The Bureau Privacy and Civil Liberties Officer(s) who certify that all requirements in TD and TD P 25-07 have been completed so a PCLIA can be reviewed and approved by the Treasury Deputy Assistant Secretary for Privacy, Transparency, and Records.

Collect (including "collection") – means the retrieval, receipt, gathering, or acquisition of any PII and its storage or presence in a Treasury system. This term should be given its broadest possible meaning.

Contractors and service providers – are private companies that provide goods or services under a contract with the Department of the Treasury or one of its Bureaus. This includes, but is not limited to, information providers, information processors, and other organizations providing information system development, information technology services, and other outsourced applications.

Data mining – means a program involving pattern-based queries, searches, or other analyses of 1 or more electronic databases, where **–** (a) a department or agency of the federal government, or a non-federal entity acting on behalf of the federal government, is conducting the queries, searches, or other analyses to discover or locate a predictive pattern or anomaly indicative of terrorist or criminal activity on the part of any individual or individuals; (b) the queries, searches, or other analyses are not subject-based and do not use personal identifiers of a specific individual, or inputs associated with a specific individual or group of individuals, to retrieve information from the database or databases; and (c) the purpose of the queries, searches, or other analyses is not solely **–** (i) the detection of fraud, waste, or abuse in a government agency or program; or (ii) the security of a government computer system.

Disclosure – When it is clear from its usage that the term "disclosure" refers to records provided to the public in response to a request under the Freedom of Information Act (5 U.S.C. § 552, "FOIA") or the Privacy Act (5 U.S.C. § 552a), its application should be limited in that manner. Otherwise, the term should be interpreted as synonymous with the terms "sharing" and "dissemination" as defined in this manual.

Dissemination – as used in this manual, is synonymous with the terms "sharing" and "disclosure" (unless it is clear from the context that the use of the term "disclosure" refers to a FOIA/Privacy Act disclosure).

E-Government – means the use of digital technologies to transform government operations to improve effectiveness, efficiency, and service delivery.

Federal information system – means a discrete set of information resources organized for the collection, processing, maintenance, transmission, and dissemination of information owned or under the control of a federal agency, whether automated or manual.

Final Rule – After the NPRM comment period closes, the agency reviews and analyzes the comments received (if any). The agency has the option to proceed with the rulemaking as proposed, issue a new or modified proposal, or withdraw the proposal before reaching its final decision. The agency can also revise the supporting analyses contained in the NPRM (e.g., to address a concern raised by a member of the public in response to the NPRM).

Government information – means information created, collected, used, maintained, processed, disseminated, or disposed of by or for the federal government.

Individual – means a citizen of the United States or an alien lawfully admitted for permanent residence. If a question does not specifically inquire about or an issue does not clearly involve a Privacy Act system of records, the term should be given its common, everyday meaning. In certain contexts, the term individual may also include citizens of other countries who are covered by the terms of an international or other agreement that involves information stored in the system or used by the project.

Information – means any representation of knowledge such as facts, data, or opinions in any medium or form, regardless of its physical form or characteristics. This term should be given the broadest possible meaning. This term includes, but is not limit to, information contained in a Privacy Act system of records.

Information technology (IT) – means any equipment or interconnected system or subsystem of equipment, used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency, if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency that requires the use: (i) of that equipment; or (ii) of that equipment to a significant extent in the performance of a service or the furnishing of a product. It includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including support services), and related resources; but does not include any equipment acquired by a federal contractor incidental to a federal contract. Clinger-Cohen Act of 1996, 40 U.S.C. § 11101(6).

Major Information system – embraces "large" and "sensitive" information systems and means "a system or project that requires special management attention because of its importance to an agency mission; its high development, operating, or maintenance costs; or its significant role in the administration of agency programs, finances, property, or other resources." OMB Circular A-130, § 6.u. This definition includes all systems that contain PII and are rated as "MODERATE or HIGH impact" under Federal Information Processing Standard 199.

National Security systems – a telecommunications or information system operated by the federal government, the function, operation or use of which involves: (1) intelligence activities, (2) cryptologic activities related to national security, (3) command and control of military forces, (4) equipment that is an integral part of a weapon or weapons systems, or (5) systems critical to the direct fulfillment of military or intelligence missions, but does not include systems used for routine administrative and business applications, such as payroll, finance, logistics, and personnel management. Clinger-Cohen Act of 1996, 40 U.S.C. § 11103.

Notice of Proposed Rule Making (NPRM) – the Privacy Act (Section (J) and (k)) allow agencies to use the rulemaking process to exempt particular systems of records from some of the requirements in the Act. This process is often referred to as "notice-and-comment rulemaking." The agency publishes an NPRM to notify the public that the agency is proposing a rule and

provides an opportunity for the public to comment on the proposal before the agency can issue a final rule.

Personally Identifiable Information (PII) –any information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual.

Privacy and Civil Liberties Impact Assessment (PCLIA) – a PCLIA is:

(1) a *process* conducted to: (a) identify privacy and civil liberties risks in systems, programs, and other activities that maintain PII; (b) ensure that information systems**,** programs, and other activities comply with legal, regulatory, and policy requirements; (c) analyze the privacy and civil liberties risks identified; (d) identify remedies, protections, and alternative or additional privacy controls necessary to mitigate those risks; and (e) provide notice to the public of privacy and civil liberties protection practices.
(2) a *document* that catalogues the outcome of that privacy and civil liberties risk assessment process.

Protected Information – as the term is used in this PCLIA, has the same definition given to that term in TD 25-10, Section 4.

Privacy Act Record – any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, the individual's education, financial transactions, medical history, and criminal or employment history and that contains the individual's name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph. 5 U.S.C. § 552a (a)(4).

Reviewing Official – The Deputy Assistant Secretary for Privacy, Transparency, and Records who reviews and approves all PCLIAs as part of her/his duties as a direct report to the Treasury Senior Agency Official for Privacy.

Routine Use – with respect to the disclosure of a record outside of Treasury (i.e., external sharing), the sharing of such record for a purpose which is compatible with the purpose for which it was collected 5 U.S.C. § 552a(a)(7).

Sharing – any Treasury initiated distribution of information to government employees or agency contractors or grantees, including intra- or inter-agency transfers or exchanges of Treasury information, regardless of whether it is covered by the Privacy Act. It does not include responses to requests for agency records under FOIA or the Privacy Act. It is synonymous with the term "dissemination" as used in this assessment. It is also synonymous with the term "disclosure" as used in this assessment unless it is clear from the context in which the term is used that it refers to disclosure to the public in response to a request for agency records under FOIA or the Privacy Act.

System – as the term used in this manual, includes both federal information systems and information technology.

System of Records – a group of any records under the control of Treasury from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual. 5 U.S.C. § 552a (a)(5).

System of Records Notice – Each agency that maintains a system of records shall publish in the *Federal Register* upon establishment or revision a notice of the existence and character of the system of records, which notice shall include: (A) the name and location of the system; (B) the categories of individuals on whom records are maintained in the system; (C) the categories of records maintained in the system; (D) each routine use of the records contained in the system, including the categories of users and the purpose of such use; (E) the policies and practices of the agency regarding storage, retrievability, access controls, retention, and disposal of the records; (F) the title and business address of the agency official who is responsible for the system of records; (G) the agency procedures whereby an individual can be notified at her/his request if the system of records contains a record pertaining to him; (H) the agency procedures whereby an individual can be notified at her/his request how she/he can gain access to any record pertaining to him contained in the system of records, and how she/he can contest its content; and (I) the categories of sources of records in the system. 5 U.S.C. § 552a (e)(4).

System Owner – Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of a system.

Section 3: System Overview

Section 3.1: System/Project Description and Purpose

The purpose of the Treasury Government Security Operations Center (GSOC) Network is to support Treasury's mission and assist in preventing, detecting, analyzing, responding, reporting on, and remediating computer security incidents throughout the Department. The Treasury GSOC Network uses personally identifiable information (PII) to identify Treasury personnel involved in GSOC cyber security investigations.

The primary sources of cyber security threats are the internet and email. GSOC has three data sources: packet capture data, system logs, and Treasury's HRConnect system.

Packet Capture (PCAP) Data

The Treasury GSOC Network receives PCAP data from the Trusted Internet Connections (TIC) used by Treasury and by a GSOC device operating at a TIC (or Bureau). The TICs provide a controlled and secure conduit whereby network data flow to/from Treasury to/from the internet. PCAP data usually are obtained by copying all data that enters the TIC over the network to another location. This copied data are called PCAP and then can be reconstructed to obtain the data streams that passed through the TIC.

PCAP data can contain email as well as other network service protocols (e.g., Domain Name Servers (DNS) and web traffic). For example, both inbound and outbound email can be captured, which would contain no more data than what is typically found on internal Treasury email servers.

PCAP data will in some cases contain PII. For instance, a member of the public could send email to a Treasury address that contains PII, such as that person's name, address, or phone number. However, the Treasury GSOC has no means to verify whether such data are authentic. Note, this example shows PII in the incoming data stream, but it could be in the outgoing data stream also.

This data provide the following types of PII referenced in Section 4.2:

- Personal email addresses of senders or recipients of email
- Business email addresses of senders or recipients of email
    - Note: the business email addresses of Treasury personnel are unique identifiers assigned to specific personnel by Treasury and its Bureaus.
- User ID of a Treasury employee accessing the internet
    - Note: the User ID of Treasury personnel are unique identifiers assigned to specific personnel by Treasury and its Bureaus.
- The date and time an action was taken.
- Internet sites and Uniform Resource Locators (URLs) of all accessed sites visited and what information the user may have exchanged with the site. Note, if the user uses a Hyper Text Transfer Protocol Secure (HTTPS) site the content of the session is encrypted and the GSOC is unable to see the information exchanged.
- The Internet Protocol (IP) addresses associated with email senders and recipients, websites, and individuals browsing the internet for all traffic that passes through the TICs. In other words, information sent to Treasury or sent by Treasury through the TIC.

<u>System Logs</u>

The Treasury GSOC Network receives TIC and specific Bureau system logs, such as those generated by firewalls, web proxies, email servers, DNS servers, intrusion detection systems, windows servers, and routers. The logs contain records of network activity and system access. In addition to the data listed above, the following data types referenced in Section 4.2 are provided:

- Files accessed

Of special note, GSOC receives alerts generated by the Bureau of Fiscal Service ("FS") Data Loss Prevention (DLP) initiative run at the TICs. These alerts include:

- Message Tracking ID – a unique number generated by the email system to track the process of an email through the system.
- Message ID – an ID assigned to the email by the initiating email system
- Sender's email address
- Recipient's email address
- Time stamp on email
- Alert type – e.g., SSN, phone number, address

The GSOC groups these alerts by Bureau and sends them to the Bureau once a day using an automated process. The Bureaus are responsible for investigating the alerts.

HRConnect Data

The Treasury GSOC obtains a data set from HRConnect for all Treasury personnel, both government employees and contractors. These data provide the following for each Treasury user:

- Name;
- Employee ID;
- Business email address; and
- Treasury organization.

These data identify individuals and their organizations whose employee IDs or business email addresses have surfaced in a cyber incident investigation. GSOC uses the data described above provided by HRConnect to investigate cyber security incidents but does not maintain or alter this file.

The following is a fictitious example describing how GSOC uses the information collected and maintained in the system:

Joe Bago Doughnuts, the name of a specific Treasury employee, received an email at his Treasury email address from MR.BAD.GUY@Gotcha.com. Joe opened the email and clicked on the embedded link, which took him to the internet site Pretty Kitten Photos. Pretty Kitten Photos is a web site for feline lovers. In addition to seeing some really cool kittens, Joe caught a very bad virus. The virus immediately started doing bad things to any computer resources Joe could access.

The GSOC used the PCAP data to determine that someone using a specific Treasury User ID accessed the questionable site Pretty Kitten Photos. The IP address of the site was a known indicator that triggered an alarm in the GSOC processing. The IP address associated with the Treasury User ID that contacted the site provided initial details about the location of the Treasury user. The date and time of the action were used to narrow the scope of the investigation and to provide a timeframe for when to search for additional information.

GSOC also used additional data provided by the various audit logs (which track user and other activities on the system) to determine how many and which files and/or systems were affected by the device with the IP address in the timeframe of the incident.

The GSOC used the Treasury email address as a search key and obtained the actual individual's name, employee ID, and organization information from HRConnect. This allowed the GSOC to notify the specific Bureau of the incident and the specifics learned. The Bureau is then responsible for investigating the incident.

From this example, GSOC would have solid information that the personal email address MR.BAD.GUY@Gotcha.com is not safe. This information is stored in an indicator database and any email received from that address in the future will create an alarm for the GSOC.

Estimated Number of Individuals Whose Personally Identifiable Information is Maintained in the System or by the Project		
☐ 0 – 999	☐ 1000 – 9,999	☐ 10,000 – 99,999
☒ 100,000 – 499,999	☐ 500,000 – 999,999	☐ 1,000,000+

Section 3.2: Authority to Collect

The authorities for operating this system or performing this project are:

- 44 U.S.C. § 3554, *Federal Information Security Modernization Act (FISMA)* - instructs the head of each federal agency to provide, "information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of (i) information collected or maintained by or on behalf of the agency; and (ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency."
- 44 U.S.C. 3534, *Federal agency responsibilities* – agency responsibilities for providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruptions, modification, or destruction of information collected or maintained by or on behalf of the agency, and information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency
- 31 U.S.C. § 321, *General authority of the Secretary* – General authorities of the Secretary of the Treasury.
- 5 U.S.C. § 301, *Departmental regulations* –regulations for the operation of the department; conduct of its employees; distribution and performance of its business; and the custody, use, and preservation of its records, papers, and property.
- Homeland Security Presidential Directive 12 (HSPD-12) – requires the development and agency implementation of a government-wide standard for secure and reliable forms of identification for federal employees and contractors.

Section 4: Information Collection

Section 4.1: Relevant and Necessary

The Privacy Act requires "each agency that maintains a system of records [to] maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be fulfilled by statute or by executive order of the President." 5 U.S.C. § 552a (e)(1). It allows federal agencies to exempt records from certain requirements (including the relevant and necessary requirement) under certain conditions5 U.S.C. §552a (k). The proposed exemption must be described in a Notice of Proposed Rulemaking ("NPRM"). In the context of the Privacy Act, the purpose of the NPRM is to give the public notice of a Privacy Act exemption claimed for a system of records and solicit public opinion on the proposed exemption. After addressing any public concerns raised in response to the NPRM, the agency must issue a Final Rule. It is possible for some, but not all, of the records maintained in the system or by the project to be exempted from the Privacy Act through the NPRM/Final Rule process.

Section 4.1(a) Please check all of the following that are true:

1. ☐ None of the PII maintained in the system or by the project is part of a Privacy Act system of records;
2. ☐ All of the PII maintained in the system or by the project is part of a system of records and none of it is

exempt from the Privacy Act relevant and necessary requirement;

3. ☐ All of the PII maintained in the system or by the project is part of a system of records and all of it is exempt from the Privacy Act relevant and necessary requirement;
4. ☐ Some, but not all, of the PII maintained in the system or by the project is part of a system of records and the records to which the Privacy Act applies are exempt from the relevant and necessary requirement; and
5. ☒ Some, but not all, of the PII maintained in the system or by the project is part of a system of records and none of the records to which the Privacy Act applies are exempt from the relevant and necessary requirement.

Section 4.1(b) ☐ Yes ☐ No ☒ N/A With respect to PII maintained in the system or by the project that is subject to the Privacy Act's relevant and necessary requirement, was an assessment conducted prior to collection (e.g., during Paperwork Reduction Act analysis) to determine which PII types (see Section 4.2 below) were relevant and necessary to meet the system's or project's mission requirements?

Section 4.1(c) ☒ Yes ☐ No ☐ N/A With respect to PII currently maintained in the system or by the project that is subject to the Privacy Act's relevant and necessary requirement, is the PII limited to only that which is relevant and necessary to meet the system's or project's mission requirements.

Section 4.1(d) ☒ Yes ☐ No With respect to PII maintained in the system or by the project that is subject to the Privacy Act's relevant and necessary requirement, is there a process to continuously reevaluate and ensure that the PII remains relevant and necessary?

In 2011, the Office of Privacy, Transparency, and Records (PTR) determined the GSOC Network did not constitute a system of records and, therefore, did not require a System of Records Notice (SORN). However, since 2011, the GSOC has incorporated a database provided by HRConnect, which contains the name, employee ID, business email address, and organization for all Treasury personnel, both government employees and contractors. GSOC uses these data to identify individuals and their organization whose employee ID or business email address surfaced in a cyber incident investigation.

Records described in the following two SORNs support this system:
Treasury .001 – Treasury Personnel and Payroll System; and
Treasury .015 – General Information Technology Access Account Records.

None of the records in the two SORNs is exempt from the relevant and necessary requirement under the Privacy Act. PTR evaluated the collection of limited information from Treasury employees and contractors and determined that the limited information is both relevant and necessary to carry out the mission of the GSOC Network.

Section 4.2: PII and/or information types or groupings

To perform their various missions, federal agencies must necessarily collect various types of information. The checked boxes below represent the types of information maintained in the system or by the project. Information identified below is used by the system or project to fulfill the purpose stated in Section 3.3 – Authority to Collect.

Biographical/General Information		
☒ Name	☐ Gender	☐ Group/Organization Membership
☐ Date of Birth	☐ Race	☐ Military Service Information
☐ Home Physical/Postal Mailing Address	☐ Ethnicity	☐ Personal Home Phone or Fax Number
☐ Zip Code	☐ Personal Cell Number	☐ Alias (including nickname)
☐ Business Physical/Postal	☐ Business Cell Number	☐ Business Phone or Fax Number

Mailing Address		
☒ Personal e-mail address	☐ Nationality	☐ Mother's Maiden Name
☒ Business e-mail address	☐ Country of Birth	☐ Spouse Information
☐ Personal Financial Information (including loan information)	☐ City or County of Birth	☐ Children Information
☐ Business Financial Information (including loan information)	☐ Immigration Status	☐ Information about other relatives.
☐ Marital Status	☐ Citizenship	☐ Professional/personal references or other information about an individual's friends, associates or acquaintances.
☐ Religion/Religious Preference	☐ Device settings or preferences (e.g., security level, sharing options, ringtones).	☐ Global Positioning System (GPS)/Location Data
☐ Sexual Orientation	☒ User names, avatars, etc.	☐ Secure Digital (SD) Card or Other Data stored on a card or other technology
☐ Cell tower records (e.g., logs. user location, time etc.)	☒ Network communications data	☐ Cubical or office number
☐ Contact lists and directories (known to contain personal information)	☐ Contact lists and directories (not known to contain personal information, but uncertain)	☐ Contact lists and directories (known to contain only business information)
☐ Education Information	☐ Resume or curriculum vitae	☐ Other (please describe):
☐ ☐ Other (please describe):	☐ Other (please describe): _____	☐ Other (please describe): _____

Identifying Numbers	
☐ Full Social Security number	☐ Health Plan Beneficiary Number
☐ Truncated/Partial Social Security number (e.g., last 4 digits)	☐ Alien Registration Number
☐ Personal Taxpayer Identification Number	☐ Business Taxpayer Identification Number (If known: ☐ sole proprietor; ☐ non-sole proprietor)
☐ Personal Credit Card Number	☐ Business Credit Card Number (If known: ☐ sole proprietor; ☐ non-sole proprietor)
☐ Personal Vehicle Identification Number	☐ Business Vehicle Identification Number (If known: ☐ sole proprietor; ☐ non-sole proprietor)
☐ Personal License Plate Number	☐ Business License Plate Number (If known: ☐ sole proprietor; ☐ non-sole proprietor)
☐ File/Case ID Number (individual)	☐ File/Case ID Number (business) (If known: ☐ sole proprietor; ☐ non-sole proprietor)
☐ Personal Professional License Number	☐ Business Professional License Number (If known: ☐ sole proprietor; ☐ non-sole proprietor)
☒ Employee Identification Number	☐ Patient ID Number
☐ Business Bank Account Number	☐ Personal Bank Account Number
☐ Commercially obtained internet navigation/purchasing habits of individuals	☐ Government obtained internet navigation/purchasing habits of individuals
☐ Business License Plate Number (non-sole-proprietor)	☐ Driver's License Number

☐ Personal device identifiers or serial numbers	☐ Other Identifying Numbers (please describe):_____
☐ Passport Number and Passport information (including full name, passport number, DOB, POB, sex, nationality, issuing country photograph and signature) (use "Other" if some but not all elements are collected)	☐ Other Identifying Numbers (please describe):_____

Medical/Emergency Information Regarding Individuals		
☐ Medical/Health Information	☐ Worker's Compensation Act Information	☐ Patient ID Number
☐ Mental Health Information	☐ Disability Information	☐ Emergency Contact Information (e.g., a third party to contact in case of emergency)
☐ Other (please describe): _____		

Biometrics/Distinguishing Features/Characteristics of Individuals		
☐ Physical description/ characteristics (e.g., hair, eye color, weight, height, sex, gender)	☐ Signatures	☐ Vascular scans
☐ Fingerprints	☐ Photos	☐ Retina/Iris Scans
☐ Palm prints	☐ Video	☐ Dental Profile
☐ Voice audio recording	☐ Scars, marks, tattoos	☐ DNA Sample or Profile
☐ Other (please describe): _____	☐ Other (please describe): _____	☐ Other (please describe): _____

Specific Information/File Types		
☐ Taxpayer Information/Tax Return Information	☐ Law Enforcement Information	☐ Security Clearance/Background Check Information
☐ Civil/Criminal History Information/Police Records (government source)	☐ Credit History Information (government source)	☐ Bank Secrecy Act Information
☐ Civil/Criminal History Information/Police Records (commercial source)	☐ Credit History Information (commercial source)	☐ National Security/Classified Information
☐ Protected Information (as defined in Treasury Directive 25-10)	☐ Case files	☐ Personnel Files
☐ Information provided under a confidentiality agreement	☐ Information subject to the terms of an international or other agreement	☐ Other (please describe): _____

Audit Log and Security Monitoring Information		
☒ User ID assigned to or generated by a user of Treasury IT	☒ Date and time an individual accesses a facility, system, or other IT	☒ Files accessed by a user of Treasury IT (e.g., web navigation habits)
☐ Passwords generated by or assigned to a user of Treasury IT	☒ Internet or other queries run by a user of Treasury IT	☐ Contents of files accessed by a user of Treasury IT
☐ Biometric information used to access Treasury facilities or IT	☐ Video of individuals derived from security cameras	☐ Public Key Information (PKI).

☒ Information revealing an individual's presence in a particular location as derived from security token/key fob, employee identification card scanners or other IT or devices	☐ Still photos of individuals derived from security cameras.	☒ Internet Protocol (IP) Address
☐ Other (please describe):	☐ Other (please describe):	☐ Other (please describe): _____

Other	
☐ Other (please describe: _____	☐ Other (please describe: _____
☐ Other (please describe: _____	☐ Other (please describe: _____

Section 4.3: Sources of information and the method and manner of collection

Packet Capture Data	System Logs	HRConnect
Specific PII identified in Section 4.2 that was acquired from this source: Personal e-mail address, Business e-mail address	**Specific PII identified in Section 4.2 that was acquired from this source:** All data shown in the Audit Log and Security Monitoring Information Table. Personal e-mail address, Business e-mail address, Network communications data	**Specific PII identified in Section 4.2 that was acquired from this source:** Name, Business e-mail address, User names, avatars etc., Employee Identification Number, User ID
Manner in which information is acquired from source by the Treasury project/system: (select all that apply):	**Manner in which information is acquired from source by the Treasury project/system: (select all that apply):**	**Manner in which information is acquired from source by the Treasury project/system: (select all that apply):**
☐ From a paper or electronic form provided to individuals, the public or members of a particular group	☐ From a paper or electronic form provided to individuals, the public or members of a particular group	☐ From a paper or electronic form provided to individuals, the public or members of a particular group
Please identify the form name (or description) and/or number (e.g., OMB Control Number): _____	Please identify the form name (or description) and/or number (e.g., OMB Control Number): _____	Please identify the form name (or description) and/or number (e.g., OMB Control Number): _____
☐ Received in paper format other than a form.	☐ Received in paper format other than a form.	☐ Received in paper format other than a form.

☐ Delivered to the project on disk or other portable device and uploaded to the system.	☐ Delivered to the project on disk or other portable device and uploaded to the system.	☐ Delivered to the project on disk or other portable device and uploaded to the system.
☐ Accessed and downloaded or otherwise acquired via the internet	☐ Accessed and downloaded or otherwise acquired via the internet	☐ Accessed and downloaded or otherwise acquired via the internet
☐ Email	☐ Email	☐ Email
☐ Scanned documents uploaded to the system.	☐ Scanned documents uploaded to the system.	☐ Scanned documents uploaded to the system.
☒ Bulk transfer	☒ Bulk transfer	☒ Bulk transfer
☐ Extracted from particular technology (e.g., radio frequency identification data (RFID) devices, video or photographic cameras, biometric collection devices).	☐ Extracted from particular technology (e.g., radio frequency identification data (RFID) devices, video or photographic cameras, biometric collection devices).	☐ Extracted from particular technology (e.g., radio frequency identification data (RFID) devices, video or photographic cameras, biometric collection devices).
☐ Fax	☐ Fax	☐ Fax
☐ Extracted from notes of a phone interview or face to face contact	☐ Extracted from notes of a phone interview or face to face contact	☐ Extracted from notes of a phone interview or face to face contact
☐ Other: Please describe: _____	☐ Other: Please describe: _____	☐ Other: Please describe: _____

Section 4.4: Privacy and/or civil liberties risks related to collection

Notice of Authority, Principal Uses, Routine Uses, and Effect of not Providing Information

When Federal agencies use a form to obtain information from an individual that will be maintained in a system of records, they must inform the individual of the following: "(A) the authority (whether granted by statute, or by executive order of the President) which authorizes the solicitation of the information and whether disclosure of such information is mandatory or voluntary; (B) the principal purpose or purposes for which the information is intended to be used; (C) the routine uses which may be made of the information as published pursuant to paragraph (4)(D) of this subsection; and (D) the effects on her/him, if any, of not providing all or any part of the requested information." 5 U.S.C § 522a (e)(3).

Section 4.4(a) ☐ Yes ☒ No Is any of the PII maintained in the system or by the project collected directly from an individual?

Section 4.4(b) ☐ Yes ☐ No ☒ N/A Was the information collected from the individual using a form (paper or electronic)?

Section 4.4(c) ☐ Yes ☐ No ☒ N/A If the answer to Section 4.4(b) was "yes," was the individual notified (on the form in which the PII was collected or on a separate form that can be retained by the individual) about the following at the point where the information was collected (e.g., in a form; on a website).

☐ The authority (whether granted by statute, or by Executive order of the President) which authorizes the solicitation of the information.
☐ Whether disclosure of such information is mandatory or voluntary.
☐ The principal purpose or purposes for which the information is intended to be used.
☐ The individuals or organizations outside of Treasury with whom the information may be/ will be shared.
☐ The effects on the individual, if any, if they decide not to provide all or any part of the requested information.

GSOC receives information from the PCAP, system logs, and HRConnect. It does not collect PII directly from any individual. HRConnect data are, however, collected directly from employees.

Treasury employees and contractors are notified each time they log onto their Treasury issued computers that their transactions on government devices are not private and are subject to review.

Use of Social Security Numbers

Social Security numbers ("SSN") are commonly used by identity thieves to commit fraudulent acts against individuals. The SSN is one data element that has the ability to harm the individual and requires more protection when used.

In addition, the Privacy Act provides that: "It shall be unlawful for any Federal, State or local government agency to deny to any individual any right, benefit, or privilege provided by law because of such individual's refusal to disclose his social security account number." Pub. L. No. 93–579, § 7. This provision does not apply to: (1) any disclosure which is required by federal statute; or (2) any disclosure of an SSN to any federal, state, or local agency maintaining a system of records in existence and operating before January 1, 1975, if such disclosure was required under statute or regulation adopted prior to such date to verify the identity of an individual. *Id.* at § 7(a)(2)(A)-(B).

Section 4.4(d) ☐ Yes ☒ No ☐ N/A Does the system or project maintain SSNs?

Section 4.4(e) ☐ Yes ☐ No ☒ N/A Are there any alternatives to the SSNs as a personal identifier? If yes, please provide a narrative explaining why other alternatives to identify individuals will not be used.

Section 4.4(f) ☐ Yes ☐ No ☒ N/A Will individuals be denied any right, benefit, or privilege provided by law because of such individual's refusal to disclose their SSN? If yes, please check the applicable box::

☐ SSN disclosure is required by Federal statute or Executive Order ; or
☐ the SSN is disclosed to any Federal, state, or local agency maintaining a system of records in existence and operating before January 1, 1975, and disclosure was required under statute or regulation adopted prior to such date to verify the identity of an individual.

Section 4.4(g) ☐ Yes ☐ No ☒ N/A When the SSN is collected, are individuals given notice whether disclosure is mandatory or voluntary, the legal authority such number is solicited, and what uses will be made of it? If yes, please explain what means are used to provide notice.

GSOC does not collect or use SSNs.

First Amendment Activities

The Privacy Act requires that Federal agencies, "maintain no record describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual about whom the record is maintained or unless pertinent to and within the scope of an authorized law enforcement activity." 5 U.S.C. § 552a(e)(7).

Section 4.4(h) ☐ Yes ☒ No Does the system or project maintain any information describing how an individual exercises their rights guaranteed by the First Amendment?

Section 4.4(h) If the system or project maintains information describing how an individual exercises their rights guaranteed by the First Amendment, do any of the following exceptions apply (the information may be maintained if any of the exceptions apply)?

☒ N/A (system or project does not maintain any information describing how an individual exercises their rights guaranteed by the First Amendment so no exceptions are needed)

☐ The individual about whom the information was collected or maintained expressly authorizes its collection/maintenance.
☐ The information maintained is pertinent to and within the scope of an authorized law enforcement activity.
☐ There is a statute that expressly authorizes its collection.

GSOC does not collect information about First Amendment activities.

Section 5: Maintenance, use, and sharing of the information

The following sections require a clear description of the system's or project's use of information.

Section 5.1: Describe how and why the system or project uses the information it collects and maintains

Please describe all of the uses of the information types and groupings collected and maintained by the system or project (see Section 4.2), including a discussion of why the information is used for this purpose and how it relates to the mission of the Bureau or office that owns the system.

The primary sources of cyber security threats are the internet and email. The mission of GSOC is preventing, detecting, analyzing, responding, reporting on, and recovering from computer security incidents throughout Treasury. To accomplish this mission, GSOC has three generic data sources: PCAP, system logs and HRConnect, which were described above in Section 3.1.

Collecting Information Directly from the Individual When Using it to Make Adverse Determinations About Them

The Privacy Act requires that Federal agencies "collect information to the greatest extent practicable directly from the subject individual when the information may result in adverse

determinations about an individual's rights, benefits, and privileges under Federal programs." 5 U.S.C. § 552a(e)(2).

Section 5.1(a) ☒ Yes ☐ No Is it possible that the information maintained in the system or by the project may be used by Treasury to make an adverse determination about an individual's rights, benefits, and privileges under federal programs (e.g., decisions about whether the individual will receive a financial benefit, get a clearance or access to a Treasury facility, obtain employment with Treasury)? **Section 5.1(b)** ☒ Yes ☐ No Is it possible that Treasury will share information maintained in the system or by the project with a third party external to the Department that will use the information to make an adverse determination about an individual's rights, benefits, and privileges under federal programs? **Section 5.1(c)** ☒ Yes ☐ No ☐ N/A If information could potentially be used to make an adverse determination about an individual's rights, benefits, and privileges under federal programs, does the system or project collect information (to the greatest extent practicable) directly from the individual?
GSOC does not make adverse determinations about individuals. The information in GSOC comes from the PCAP, system logs, and HRConnect. The GSOC passes processed data and uncovered indicators of potential issues to the respective Bureau for investigation. The Bureau investigation may lead to an adverse determination. Any adverse determination would be made based on the data from the original system of record, which would be the TIC or Bureau that provided the PCAP or system log information.

Data Mining

As required by Section 804 of the Implementing the 9/11 Commission Recommendations Act of 2007 ("9-11 Commission Act"), Treasury reports annually to Congress on its data mining activities. For a comprehensive overview of Treasury's data mining activities, please review the Department's Annual Privacy reports available at: http://www.treasury.gov/privacy/annual-reports.

Section 5.1(d) ☐ Yes ☒ No Is information maintained in the system or by the project used to conduct "data-mining" activities as that term is defined in the Implementing the 9-11 Commission Act?
The "data mining" performed by the GSOC is solely for the security of Treasury's computer systems; therefore, it is excluded from the Federal Agency Data Mining Reporting Act of 2007, 42 U.S.C. § 2000ee-3 (b)(1)(C)(ii).

Section 5.2: Ensuring accuracy, completeness, and timeliness of information collected, maintained, and shared

Exemption from Accuracy, Relevance, Timeliness, and Completeness Requirements

The Privacy Act requires that Federal agencies "maintain all records which are used by the agency in making any determination about any individual with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination." 5 U.S.C § 552a(e)(5). If a particular system of records meets certain requirements (including the NPRM process defined in Section 2 above), an agency may exempt the system of records (or a portion of the records) from this requirement.

Section 5.2(a) ☐ Yes ☒ No Is all or any portion of the information maintained in the system or by the project: (a) part of a system of records and (b) exempt from the accuracy, relevance, timeliness, and completeness requirements in sections (e)(5) of the Privacy Act?
None of the information maintained in the system is both part of a system of records and exempt from the accuracy,

relevance, timeliness, and completeness requirements of the Privacy Act.

Computer Matching

The Computer Matching and Privacy Protection Act of 1988 amended the Privacy Act imposing additional requirements when Privacy Act systems of records are used in computer matching programs.

Pursuant to the Privacy Act, as amended, there are two distinct types of matching programs. The first type of matching program involves the computerized comparison of two or more automated federal personnel or payroll systems of records or a system of federal personnel or payroll records with non-federal records. This type of matching program may be conducted for any purpose. The second type of matching program involves the computerized comparison of two or more automated systems of records or a system of records with non-federal records. The purpose of this type of matching program must be for the purpose of eligibility determinations or compliance requirements for applicants, recipients, beneficiaries, participants, or providers of services for payments or in-kind assistance under federal benefit programs, or recouping payments or delinquent debts under such federal benefit programs. *See* 5 U.S.C. § 522a(a)(8).

Matching programs must be conducted pursuant to a matching agreement between the source and recipient agencies. The matching agreement describes the purpose and procedures of the matching **and** establishes protections for matching records.

Section 5.2(b) ☐ Yes ☒ No Is any of the information maintained in the system or by the project (a) part of a system of records and (b) used as part of a matching program?
Section 5.2(c) ☐ Yes ☐ No ☒ N/A Is there a matching agreement in place that contains the information required by Section (o) of the Privacy Act?
Section 5.2(d) ☐ Yes ☐ No ☒ N/A Are assessments made regarding the accuracy of the records that will be used in the matching program?
Section 5.2(e) ☐ Yes ☐ No ☒ N/A Does the Bureau or office that owns the system or project independently verify the information, provide the individual notice and an opportunity to contest the findings, or obtain Data Integrity Board approval in accordance with Section (p) of the Privacy Act before taking adverse action against the individual?

The GSOC data is not a part of a Computer Matching Program.

Ensuring Fairness in Making Adverse Determinations About Individuals

Federal agencies are required to, "maintain all records which are used by the agency in making any determination about any individual with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination." 5 U.S.C. § 552a(e)(5). This requirement also applies when merging records from two or more sources where the merged records are used by the agency to make any determination about any individual.

Section 5.2(f) ☐ Yes ☒ No With respect to the information maintained in the system or by the project, are steps taken to ensure all information used to make a determination about an individual is maintained with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination?

GSOC does not make adverse determinations about individuals. The information in GSOC comes from the PCAP, system logs and HRConnect. The GSOC passes processed data and uncovered indicators of potential issues to the respective Bureau for investigation. The Bureau investigation may lead to an adverse determination. Any adverse determination would be made based on the data from the original system of record, which would be the TIC or Bureau that provided the PCAP or system log information.

GSOC generates an initial report for the Bureau documenting the potential problem. If the Bureau determines an incident has occurred the GSOC will report the status up the chain, both internally to Treasury and to United States Computer Emergency Readiness Team (US-CERT). The report focuses on cyber security incidents, their impact and remediation. While a person is generally the starting point, e.g., hit a bad website or clicked on a bad email link, GSOC reports focus on what happened after that. For example: The infected computer did this; it called home; it infected another computer; it sent data from point a to point b; the fix action was, etc.

Merging Information About Individuals

Section 5.2(g) ☒ Yes ☐ No Is information maintained in the system or by the project merged with electronic or non-electronic information from internal or external sources (e.g., other files or systems)?

Section 5.2(h) ☒ Yes ☐ No ☐ N/A Once merged, is the information used in making determinations about individuals (e.g., decisions about whether the individual will receive a financial benefit or payment, get a clearance or access to a Treasury facility, obtain employment with Treasury, etc.)?

Section 5.2(i) ☐ Yes ☐ No ☒ N/A Are there documented policies or procedures for how information is merged?

Section 5.2(j) ☐ Yes ☐ No ☒ N/A Do the documented policies or procedures address how to proceed when partial matches (where some, but not all of the information being merged matches a particular individual) are discovered after the information is merged?

Section 5.2(k) ☐ Yes ☐ No ☒ N/A If information maintained in the system or by the project is used to make a determination about an individual, are steps taken to ensure the accuracy, relevance, timeliness, and completeness of the information as is reasonably necessary to assure fairness to the individual?

Individuals must authenticate their ID to log onto a Treasury computer, and everything viewed on the Treasury computer is linked to the individual user by employee ID and/or email address. GSOC receives information from the PCAP, system log, or HRConnect. GSOC does not make adverse determinations about individuals. GSOC passes processed data and uncovered indicators of potential issues to the respective Bureau for investigation. The Bureau investigation may lead to an adverse determination. Any adverse determination would be made based on the data from the original system of record, which is the TIC or Bureau that provided the PCAP or system log information.

Policies and Standard Operating Procedures or Technical Solutions Designed to Ensure Information Accuracy, Completeness, and Timeliness

Section 5.2(l) ☐ Yes ☐ No ☒ N/A If information maintained in the system or by the project is used to make any determination about an individual (even if it is an exempt system of records), are there documented policies or standard operating procedures for the system or project that address the accuracy, completeness, and timeliness of the information?

Section 5.2(m) ☐ Yes ☒ No Does the system or project use any software or other technical solutions designed to improve the accuracy, completeness, and timeliness of the information used to make an adverse determination about an individual's rights, benefits, and/or privileges (regardless of if it is an exempt system of records)?

GSOC does not make adverse determinations about individuals. The information in GSOC comes from the

PCAP, system log, or HRConnect. GSOC may process data and uncover potential issues that may lead to an adverse determination. Any adverse determination would be made based on the data from the original system of record, which is the TIC or Bureau that provided the PCAP or system log information.

Accuracy, Completeness, and Timeliness of Information Received from the Source

Section 5.2(n) ☐ Yes ☐ No ☒ N/A Did Treasury or the Bureau receive any guarantee, assurance, or other information from any information source(s) regarding the accuracy, timeliness and completeness of the information maintained in the system or by the project?

Only Treasury system devices producing logs (may be operated under contract to a contractor) and PCAP data are collected.

There are three types of data accuracy to consider: 1) the accuracy by which the system devices log the events for which they were designed, 2) the accuracy by which the packet capture device copies the network packets passing by it, and 3) the accuracy of the data sent within the packets themselves.

In a sense, the GSOC systems represent a wiretap on inbound/outbound network traffic to/from the Treasury TICs. As long as the wiretap is working as intended, the first two types of accuracy are maintained. If false information is passed through the wiretap, the third type of accuracy is violated; however, the first two types of accuracy are still maintained. The Treasury GSOC process only requires accuracy of the first two types.

To ensure data accuracy of the first type, the Treasury GSOC correlates the data with itself and with other sources such as incident data from Bureaus. GSOC will detect inaccurate data (e.g., due to system logging issues), and work toward making them accurate. This may entail working with a vendor to release a patch so that the system logs accurately.

In the second type, the data sent to the device is inaccurate. For example, this type of data would be spoofed email sender addresses (typical in spam) or false email content such as someone providing fake PII. The Treasury GSOC does not verify this information for accuracy because it is irrelevant to the Treasury GSOC's security mission and is impossible to do.

The Treasury GSOC performs analysis on the data. Part of this analysis is looking for gaps where the system logs and PCAP data are incomplete. If incomplete data are found, the Treasury GSOC asks for a retransmission of system logs or PCAP data and, if available, uses the new data to fill in the gaps.

All system log and PCAP data have date timestamps for each event. The Treasury GSOC generally receives all data feeds within 24 hours of the actual event. Data received within 24 hours are current enough for the Treasury GSOC to take action.

The Treasury GSOC receives live feeds and batch feeds of data throughout the day. If these feeds stop, the GSOC immediately attempts to identify and rectify the issue. In most cases, data can be restored over the outage periods.

System log data and PCAP data record events as they happen and, as an historical record, cannot be "out of date."

Disseminating Notice of Corrections of or Amendments to PII

Section 5.2(o) ☐ Yes ☒ No ☐ N/A Where feasible and appropriate, is there a process in place for disseminating corrections of or amendments to the PII maintained in the system or by the project to all internal and external information-sharing partners?

Section 5.2(p) ☐ Yes ☐ No ☒ N/A Where feasible and appropriate, does the process for disseminating corrections or amendments include notifying the individual whose information is corrected or amended?

The GSOC acts on PCAP and system log data. This data simply reflect exactly what transpired at a specific time. In other words, this set of characters was sent from here to there at this time. Any attempt to modify these data would corrupt and invalidate them.

Section 5.3: Information sharing within the Department of the Treasury

Internal Information Sharing
Section 5.3(a) ☒ Yes ☐ No Is PII maintained in the system or by the project shared with other Treasury Bureaus? **Section 5.3(b)** ☒ Yes ☐ No Does the Treasury Bureau or office that receives the PII limit access to those Treasury officers and employees who have a need for the PII in the performance of their official duties (i.e., those who have a "need to know")?
Bureaus *GSOC provides information to Bureau security organizations to notify them about a potential cyber security incident and/or by request.* *Bureaus may request information about specific indicators of compromise (IOC)[1], targets[2], and content information.[3] This is generally handled through the Trouble Ticket workflow. All of the information provided by the GSOC to the Bureau is the Bureau's information, which the GSOC has received and processed. GSOC will not share Bureau data with other Bureaus, Bureaus will only receive data associated with their Bureau; however, IOCs (containing no PII) will be shared across all Bureaus.* *The GSOC has incorporated a database provided by HRConnect containing the name, employee ID, business email address, and organization for all Treasury personnel, both government employees and contractors. This data is used to identify individuals and their organization whose employee ID or business email address surfaced in a cyber incident investigation. This information is then used to notify Bureaus that a member of their organization has been identified in a potential cyber security incident. The data is also used to identify any individuals that seem to be targets of cyberattacks due to the fact that their email address is showing up in numerous attack vectors.* *The GSOC will not provide any information directly to an individual or supervisor. The GSOC will work with the Bureau Security or Inspector General (IG) functions to satisfy these requests. The Bureau/IG will validate the need for the requested data.* *The GSOC sends data to the Bureau's Computer Security Incident Response Center (CSIRC). There are specific guidelines in Treasury Directive Publication 85-01, Department of the Treasury Information Technology (IT) Security Program, that discusses handling PII. Access by Bureau personnel is the responsibility of the Bureau. Access by GSOC personnel is controlled by roles and permissions that provide access to the systems that contain data, and GSOC personnel must be granted access to individual GSOC systems.* ***Treasury Office of the Inspector General (OIG) and Treasury Inspector General for Tax Administration (TIGTA)*** *The GSOC has a standing relationship with the OIG and TIGTA and will provide IOCs, targets, and content information when requested. This is coordinated with the Bureau involved in the investigation. There is no*

[1] An IOC is an artifact observed on a network or in an operating system that with high confidence indicates a computer intrusion. Typical IOCs are virus signatures, IP addresses, MD5 hashes, URLs, domains, and sender email addresses.
[2] Information that indicates who in Treasury was the target of an attack. This could be a list of recipients of an email, a list of individuals who went to an infected site, or the list of individuals that were compromised. This information would only contain the individuals name and/or email address and is not routinely shared.
[3] Detailed information involved in an incident, i.e., the actual content of an email or web session. This information is not shared routinely.

formal request process established and requests are generally handled via email.

Insider Threat Program (ITP)[4]
Only the Office of Intelligence and Analysis, Office of Counter Intelligence (OIA/CI) staff can request data for the Insider Threat Program (ITP). The GSOC assumes CI staff will only send requests for which they have an appropriate case/inquiry/investigation. These requests require approval from the Office of General Counsel (OGC) and PTR. When requested, GSOC will provide web browsing history, email history without content, full email content with/without attachments, and calendar data. This program is currently limited to only Treasury personnel with a clearance.

Memorandum of Understanding/Other Agreements Limiting Treasury's Internal Use/Disclosure of PII

Section 5.3(c) ☒ Yes ☐ No ☐ N/A Is any of the PII maintained in the system or by the project subject to the requirements of a Memorandum of Understanding (MOU) or other agreement (e.g., agreement with another federal or state agency that provided the information to the Treasury or subject to an international agreement or treaty) that limits or places conditions on Treasury's internal use, maintenance, handling, or disclosure of the PII?

The GSOC has established a MOU and an Information Security Agreement (ISA) with FS that address the data provided by the FS TICs to the GSOC.

Internal Information Sharing Chart

Internal Recipient's Name (e.g., Bureau or office)	Bureau CSIRCs	OIG and TIGTA	ITP
Purpose of the Sharing	Cyber Security Awareness	Cyber Security Awareness	Cyber Security Awareness/ Investigations
PII Shared	User ID Name Email address IP addresses Content of emails or web sessions	User ID Name Email address IP addresses Content of emails or web sessions	User ID Name Email address IP addresses web browsing history, email history without content, full email content with/without attachments, and calendar data
Applicable Statutory or Regulatory or Restrictions on Information Shared	None	None	None
Applicable Restrictions Imposed by Agreement on Information Shared (e.g., by Treasury agreement with the party that provided the information to Treasury)	None	None	Limited to OIA/CI staff with OGC and PTR approval

[4] Treasury established the Insider Threat Program in accordance with Executive Order 13587 to deter, detect, and mitigate insider threats that would do harm to the security of the United States. These efforts include safeguarding classified national security information, while protecting the privacy, civil rights, and civil liberties of Treasury personnel. For more information, please see: https://www.treasury.gov/about/role-of-treasury/orders-directives/Pages/to105-20.aspx.

Name and Description of MOU or Other Agreement Restricting Treasury's Internal Use, Maintenance, Handling, or Sharing of PII Received	MOU and ISA with FS	N/A	N/A
Method of PII Transfer (e.g., paper/oral disclosures/magnetic disk/portable device/email/fax/other (please describe if other)	Digital transmission.	Email	Form
The data provided in the PCAP provided by the TICs can contain email content or attachments with PII. The MOU with FS specifically states these data, "must not be revealed to unauthorized persons." GSOC does not share these data.			

Section 5.4: Information sharing with external (i.e., outside Treasury) organizations and individuals

External Information Sharing

Section 5.4(a) ☒ Yes ☐ No Is PII maintained in the system or by the project shared with agencies, organizations, or individuals external to Treasury?

Federal Bureau of Investigation (FBI)
The GSOC has a standing relationship with the FBI and provides indicators of compromise when requested. Target lists and email content information is not provided routinely. A GSOC member has been identified to liaise with the FBI and coordinate the routine information request process.

The FBI can request additional information related to inbound suspect emails. Any information provided would be associated strictly with these specific emails and not inclusive of the user's personal or business communications. In these cases, the GSOC will work through the OIG or TIGTA to coordinate transmission of recipient lists and email content.

Other Government Agencies
It is reasonable to assume other government agencies, including Congress examining the issues surrounding particular Treasury issues, may request additional data from Treasury. In these cases, the GSOC will assist and coordinate via OIG or TIGTA.

Accounting of Disclosures

Section 5.4(b) ☒ Yes ☐ No ☐ N/A With respect to records maintained in the system or by the project that are subject to the Privacy Act, do you maintain a paper or electronic log or other record of the date, nature, and purpose of each disclosure (not including intra-agency disclosures and FOIA disclosures) of a record to any person or to another agency (outside of Treasury) and the name and address of the person or agency to whom the disclosure is made? *See* 5 U.S.C § 552a(c).

Section 5.4(c) ☐ Yes ☐ No ☒ N/A If you do not keep a running tabulation of every disclosure at the time it is made, are you able to reconstruct an accurate and complete accounting of disclosures so as to be able to respond to Privacy Act requests in a timely fashion?

Section 5.4(d) ☒ Yes ☐ No ☐ N/A With respect to records maintained in the system or by the project that are subject to the Privacy Act, do you retain the log or other record of the date, nature, and purpose of each disclosure, for at least five years or the life of the record, whichever is longer, after the disclosure for which the accounting is made?

Section 5.4(e) ☐ Yes ☒ No ☐ N/A With respect to records maintained in the system or by the project that are subject to the Privacy Act, does your Bureau or office exempt the system of records (as allowed by the Privacy Act in certain circumstances) from the requirement to make the accounting available to the individual named in the record?

Section 5.4(f) ☐ Yes ☒ No ☐ N/A With respect to records maintained in the system or by the project that are subject to the Privacy Act, does your Bureau or office exempt the system of records (as allowed by the Privacy Act in certain circumstances) from the requirement to inform any person or other agency about any correction or notation of dispute made by the agency of any record that has been disclosed to the person or agency if an accounting of the disclosure was made?
GSOC shares limited PII with agencies, organizations, or individuals external to Treasury. GSOC has a trouble ticket database that documents disclosures outside Treasury.

Statutory or Regulatory Restrictions on Disclosure

Section 5.4(g) ☐ Yes ☒ No In addition to the Privacy Act, are there any other statutory or regulatory restrictions on the sharing of any of the PII maintained in the system or by the project (e.g., 26 U.S.C § 6103 for tax returns and return information)?
No additional statutes or regulations restrict GSOC disclosure of PII for cyber security purposes.

Memorandum of Understanding Related to External Sharing

Section 5.4(h) ☐ Yes ☒ No ☐ N/A Has Treasury (including Bureaus and offices) executed a Memorandum of Understanding, or entered into any other type of agreement, with any external agencies, organizations, or individuals with which/whom it shares PII maintained in the system or by the project?
GSOC does not have an MOU with any external agencies, organizations, or individuals.

Memorandum of Understanding Limiting Treasury's Use or Disclosure of PII

Section 5.4(i) ☐ Yes ☒ No Is any of the PII maintained in the system or by the project subject to the requirements of a Memorandum of Understanding or other agreement (e.g., agreement with another federal or state agency, an international agreement or treaty, or contract with private vendor that provided the information to Treasury or one of its Bureaus) that limits or places conditions on Treasury's internal use or external (i.e., outside Treasury) sharing of the PII?
The GSOC does not have an associated MOU.

Memorandum of Understanding Limiting External Party's Use or Disclosure of PII

Section 5.4(j) ☐ Yes ☒ No Is any of the PII maintained in the system or by the project subject to the requirements of a Memorandum of Understanding or other agreement in which Treasury limits or places conditions on an external party's use, maintenance, handling, or disclosure of PII shared by Treasury?
GSOC does not have an MOU to limit an external party's use or disclosure of PII.

External Information Sharing Chart

Section 5.4(k) ☒ Yes ☐ No Is information from the system or project shared externally?

External Recipient's Name	FBI	Other Government Agencies
Purpose of the Sharing	Cyber Security Awareness/ Investigations	Cyber Security Awareness/ Investigations
PII Shared	Name Email address Content of emails	
Applicable Statutory or Regulatory or Restrictions on Information Shared	None	None
Applicable Restrictions Imposed by Agreement on Information Shared (e.g., by Treasury agreement with the party that provided the information to Treasury)	Coordinate via OIG or TIGTA	Coordinate via OIG or TIGTA
Name and Description of MOU or Other Agreement Restricting Treasury's Internal Use, Maintenance, Handling, or Sharing of	None	None

PII Received		
Method of PII Transfer (e.g., paper/oral disclosures/magnetic disk/portable device/email/fax/other (please describe if other)	Encrypted email/ and or mail/hand delivery of encrypted digital media.	Encrypted email/ and or mail/hand delivery of encrypted digital media.

Obtaining Consent Prior to New Disclosures Not Included in the SORN or Authorized by the Privacy Act
Section 5.4(l) ☒ Yes ☐ No ☐ N/A Is the individual's consent obtained, where feasible and appropriate, prior to any **new** disclosures of previously collected records in a system of records (those not expressly authorized by the Privacy Act or contained in the published SORN (e.g., in the routine uses))?
The GSOC only makes disclosures consistent with the applicable SORNs. Individual consent will be obtained if additional disclosures inconsistent with the purpose of the original collection are ever contemplated.

Section 6: Compliance with federal information management requirements

Responses to the questions below address the practical, policy, and legal consequences of failing to comply with one or more of the following federal information management requirements (to the extent required) and how those risks were or are being mitigated: (1) the Privacy Act System of Records Notice Requirement; (2) the Paperwork Reduction Act; (3) the Federal Records Act; (4) the E-Gov Act security requirements; and (5) Section 508 of the Rehabilitation Act of 1973.

Section 6.1: Privacy Act System of Records Notice (SORN)

For collections of PII that meet certain requirements, the Privacy Act requires that the agency publish a SORN in the *Federal Register*.

System of Records
Section 6.1(a) ☒ Yes ☐ No Does the system or project retrieve records about an individual using an identifying number, symbol, or other identifying particular assigned to the individual? (see items selected in Section 4.2 above) **Section 6.1(b)** ☒ Yes ☐ No ☐ N/A Was a SORN published in the *Federal Register* for this system of records?
PII is used to identify personnel within Treasury who have been involved in a GSOC cyber security investigation. PII is retrieved from the HR records provided for GSOC to use by searching for an email address or User ID that has been found in the PCAP or system log data provided by FS. *The SORNs are:* *Treasury .001 – Treasury Personnel and Payroll System; and* *Treasury .015 – General Information Technology Access Account Records.*

Section 6.2: The Paperwork Reduction Act

The PRA requires OMB approval before a Federal agency may collect standardized data from 10 or more respondents within a 12 month period. OMB requires agencies to conduct a PIA (a Treasury PCLIA) when initiating, consistent with the PRA, a new electronic collection of PII for

10 or more persons (excluding agencies, instrumentalities, or employees of the federal government).

Paperwork Reduction Act Compliance
Section 6.2(a) ☐ Yes ☒ No Does the system or project maintain information obtained from individuals and organizations who are not federal personnel or an agency of the federal government (i.e., outside the federal government)? **Section 6.2(b)** ☐ Yes ☐ No ☒ N/A Does the project or system involve a new collection of information in identifiable form for 10 or more persons from outside the federal government? **Section 6.2(c)** ☐ Yes ☐ No ☐ N/A Did the project or system complete an Information Collection Request ("ICR") and receive OMB approval?
The Paperwork Reduction Act does not apply, because the GSOC does not collect information, PII or otherwise, from any individual.

Section 6.3: Records Management - NARA/Federal Records Act Requirements

Records retention schedules determine the maximum amount of time necessary to retain information in order to meet the needs of the project or system. Information is generally either disposed of or sent to the NARA for permanent retention upon expiration of this period.

NARA Records Retention Requirements
Section 6.3(a) ☒ Yes ☐ No Are the records used in the system or by the project covered by NARA's General Records Schedules ("GRS") or Treasury/Bureau Specific Records Schedule (SRS)? **Section 6.3(b)** ☒ Yes ☐ No Did NARA approved a retention schedule for the records maintained in the system or by the project? **Section 6.3(c)** ☐ Yes ☐ No ☒ N/A If NARA did not approve a retention schedule for the records maintained in the system or by the project and the records are not covered by NARA's GRS or Treasury/Bureau SRS, has a draft retention schedule (approved by all applicable Treasury and/or Bureau officials) been developed for the records used in this project or system?
GRS 3.2-020. Computer security incident handling, reporting and follow-up records.

Section 6.4: E-Government Act/NIST Compliance

The completion of Federal Information Security Management Act ("FISMA") Security Assessment & Authorization (SA&A) process is required before a federal information system may receive Authority to Operate ("ATO"). Different security requirements apply to National Security Systems.

Federal Information System Subject to FISMA Security Assessment and Authorization
Section 6.4(a) ☒ Yes ☐ No ☐ N/A Is the system a federal information system subject to FISMA requirements? **Section 6.4(b)** ☒ Yes ☐ No ☐ N/A Has the system or project undergone a SA&A and received ATO?

Access Controls and Security Requirements

Section 6.4(c) ☒ Yes ☐ No Does the system or project include access controls to ensure limited access to information maintained by the system or project?

Only Treasury GSOC personnel who have both passed a Treasury security background investigation and possess at least a secret security clearance (or interim secret clearance) will have read access to the data. Treasury GSOC personnel who have passed just the Treasury security background investigation may only have access to reports generated from the data.

The Treasury GSOC is comprised of about 40 individuals of basically four types: managers, developers, administrators, and analysts. Managers need read access to the data to exercise their role in mission oversight. Developers are responsible for creating and maintaining the applications that receive the data and make them available via a web front end. They need full access to the data. Administrators are responsible for the systems the data reside upon. They will have full access to the data. Analysts are responsible for using the data in their role of preventing, identifying, managing, analyzing, and recovering from Treasury security incidents. They will have read access to the data.

First, only Treasury GSOC personnel who have the appropriate clearance and Treasury background investigation are allowed read access. Second, GSOC personnel are informed on the appropriate use of system. Third, all GSOC personnel must identify and authenticate themselves to the system prior to gaining access.

All the contractors involved with the GSOC have passed Treasury background investigations and those that perform development and maintenance have at least a secret security clearance. The contractors operate in a network subject to Treasury policy and in a system that requires Treasury certification and accreditation with a security categorization of "high."

Security Risks in Manner of Collection

Section 6.4(d) ☐ Yes ☒ No In Section 4.3 above, you identified the sources for information used in the system or project and the method and manner of collection. Were any security, privacy, or civil liberties risks identified with respect to the manner in which the information is collected from the source(s)?

PTR has identified a potential risk that the individual does not receive notice of the GSOC's collection, maintenance, and use of Treasury employee data because the GSOC does not collect information directly from the individual. This risk is mitigated because Treasury employees and contractors are provided with notice each time they log onto their Treasury issued computers. In addition, notice is also provided through this PCLIA and in the SORNs referenced in Section 6.1.

Another potential risk is that there is not an MOU with the FBI. This risk is mitigated because there are limits to the information shared with the FBI. However, GSOC would benefit from a written procedure that outlines the limits to sharing with the FBI and other outside agencies. The GSOC will work with PTR to establish and document a policy for external disclosures that further mitigates this risk before the next iteration of the PCLIA is published.

Security Controls When Sharing Internally or Externally

Section 6.4(e) ☒ Yes ☐ No ☐ N/A Are all Treasury/Bureau security requirements met in the method of transferring information (e.g., bulk transfer, direct access by recipient, portable disk, paper) from the Treasury project or system to internal or external parties?

All information transmitted between parties is fully encrypted in transmission. No user has access to information without authentication and authorization.

Monitoring of Individuals

Section 6.4(f) ☒ Yes ☐ No Will this system or project have the capability to identify, locate, and monitor individuals or groups of people?

The system provides the capability of monitoring inbound/outbound network traffic and email at the Treasury's TIC. This provides the GSOC, in some cases, the ability to monitor inbound/outbound traffic and the email sent by or received by Treasury personnel. Treasury personnel can be identified specifically by comparing their user ID, employee ID, or business email address to the data provided by HRConnect. *The system does not provide the ability to locate individuals, unless an individual deliberately sends content through the Treasury network providing updates about their location.* *The Treasury GSOC is a small organization. No non-Treasury GSOC personnel have any type of access to the Treasury GSOC systems containing PCAP data, system log data, or analysis data. Each Treasury GSOC individual who has full access to the data has passed a Treasury background investigation and holds at least a secret security clearance. The system requires identification and authentication prior to granting user access. Personnel are trained on the appropriate use of the system.*

Audit Trails
Section 6.4(g) ☐ Yes ☒ No Are audit trails regularly reviewed for appropriate use, handling, and disclosure of PII maintained in the system or by the project inside or outside of the Department?
There are no audit trails specifically intended to monitor the use, handling, or disclosure of PII within GSOC. However, the GSOC does ingest a very large amount of data that can be mined and used as a forensic tool to determine who took, or more specifically what user account or IP address was used for, a specific action with regards to the movement of PII and the extent of the PII involved.

Section 6.5: Section 508 of the Rehabilitation Act of 1973

When Federal agencies develop, procure, maintain, or use Electronic and Information Technology ("EIT"), Section 508 of the Rehabilitation Act of 1973 (as amended in 1998) requires that individuals with disabilities (including federal employees) must have access and use (including privacy policies and directives as well as redress opportunities) that is comparable to that which is available to individuals who do not have disabilities.

Applicability of and Compliance With the Rehabilitation Act
Section 6.5(a) ☒ Yes ☐ No Will the project or system involve the development, procurement, maintenance or use of EIT as that term is defined in Section 508 of the Rehabilitation Act of 1973 (as amended in 1998)? **Section 6.5(b)** ☐ Yes ☒ No ☐ N/A Does the system or project comply with all Section 508 requirements, thus ensuring that individuals with disabilities (including federal employees) have access and use (including access to privacy and civil liberties policies) that is comparable to that which is available to individuals who do not have disabilities?
There has been no attempt made to design the GSOC to be 508 compliant and the GSOC has not executed a Voluntary Product Accessibility Template (VPAT) assessment. This could change if GSOC hired an individual with special needs.

Section 7: Redress

Access Under the Freedom of Information Act and Privacy Act
Section 7.0(a) ☒ Yes ☐ No Does the agency have a published process in place by which individuals may seek records under the Freedom of Information Act (FOIA) and Privacy Act (PA)?
The Treasury/Bureaus FOIA and PA disclosure regulations can be found at 31 C.F.R. Part 1, Subtitle A, Subparts A and C.

Privacy Act Access Exemption

Section 7.0(b) ☐ Yes ☒ No Was any of the information that is maintained in system of records and used in the system or project exempted from the access provisions of the Privacy Act?
The system is not exempt from the access provisions of the Privacy Act.

Additional Redress Mechanisms

Section 7.0(c) ☐ Yes ☒ No With respect to information maintained by the project or system (whether or not it is covered by the Privacy Act), does the Bureau or office that owns the project or system have any additional mechanisms other than Privacy Act and FOIA remedies (e.g., a customer satisfaction unit; a complaint process) by which an individual may request access to and/or amendment of their information and/or contest adverse determinations about denial of their rights, benefits, and privileges under federal programs (e.g., decisions about whether the individual will receive a financial benefit, get a clearance or access to a Treasury facility, obtain employment with Treasury)?
There are no additional redress mechanisms. The information in GSOC comes from the PCAP, system logs, or HRConnect. The data from the PCAP and system log reflect exactly what transpired at a specific time. Any attempt to modify these data would corrupt and invalidate the data. Individuals can access data through the HRConnect system to update their data throughout their employment. However, any data that GSOC processes that uncovers indicators of potential issues is passed to the respective Bureau and the Bureau investigation may lead to an adverse determination. Any adverse determination is carried out by the Bureau and the Bureau is responsible for providing Privacy Act and Freedom of Information Act records and redress.