Privacy and Civil Liberties Impact Assessment
for the

CORONAVIRUS DISEASE 19 (COVID-19) BODY TEMPERATURE SCREENING PROGRAM

October 28, 2020

Bureau Reviewing Official
Togai Andrews
Chief, Office of Critical Infrastructure and IT Security
Office of the Chief Information Officer
Bureau of Engraving and Printing
Department of the Treasury

Bureau Privacy Official
Anthony Johnson
Government Information Specialist (Privacy)
Office of Critical Infrastructure and IT Security
Cyber Security Policy and Compliance Division
Bureau of Engraving and Printing
Department of the Treasury

Section 1: Introduction

To protect the health and safety of all individuals within the Bureau of Engraving and Printing (BEP) facilities against the spread of the Coronavirus Disease 2019 ("COVID-19"), the BEP will measure the body temperature of BEP employees and contractors, non-BEP Federal government employees and contractors, and members of the public ("COVID-19 Body Temperature Screening Program") prior to entering the Washington, D.C. Facility ("DCF") and the Western Currency Facility ("WCF"). DCF employees and contractors of the Office of Environmental Health and Safety and the WCF Police Officers of the Office of Manufacturing Support, Security Division ("Screeners") will administer the COVID-19 Body Temperature Screening Program.

BEP is preparing this PCLIA to provide transparency into a program that impacts individuals, including members of the public, by collecting biometric information (the body temperature reading), which is medical information. Therefore, the body temperature reading is considered Personally Identifiable Information (PII). Although the body temperature reading and the fact that the individual has an elevated temperature is medical information that constitute PII, neither the Screeners nor the technology will retain the PII in any form after conducting the screening.

Additionally, this PCLIA also provides transparency into potential PII collection by supervisors following the denied entry of a BEP employee only as they communicate and manage medical information, work statuses, and leave accounting activities. This PCLIA does not address any contact tracing activities related to COVID-19.

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 BEP administers the COVID-19 Body Temperature Screening Program ("Program") to measure the body temperatures of all individuals prior to granting entrance into the Washington, D.C. Facility ("DCF") and the Western Currency Facility ("WCF"). Screeners will measure body temperatures using BEP designated non-invasive/non-contact/no-touch infrared thermometers or thermographic imaging cameras as described below. BEP will ensure the *COVID-19 Body Temperature Screening Program Notice* is highly visible to the individuals and near the collection site before commencing body temperature screening activities. (See Attachment I). This Notice explains the effects of the Program to individuals.

If the individual's body temperature registers below 100.4˚F, the Screener will allow the individual to enter the facility. The Screener may display or communicate verbally (in a low-pitched/discreet voice) the temperature if requested by the individual only. No further action is required from the Screener. If an individual registers a temperature of 100.4˚F or above ("elevated temperature"), the Screener will display or communicate verbally the temperature to the individual in a discreet manner to mitigate other individuals from becoming aware of the elevated temperature. The Screener will perform a second screening to ensure that the elevated temperature was not caused by external factors.

If the individual registers a second elevated temperature, the Screener will display or communicate verbally (in a low-pitched/discreet voice) the temperature to the individual only, and will deny entry to the facility. Screeners will provide the written *COVID-19 Elevated Temperature Screening Notice to Individuals* registering a second elevated temperature with specific medical and personnel guidance. (See Attachment II). This Notice advises non-BEP Federal employees and contractors, BEP contractors, and members of the public that BEP will not record elevated temperature in any format, and will be re-screened each time they seek access to BEP. Additionally, this Notice provides the required Privacy Act Statement to BEP employees. The Screener shall not record any information such as name, body temperature, signs of flushed cheeks or fatigue, coughing or shortness of breath, or any other identifying information.

If any individual refuses to submit to body temperature screening by BEP, the individual will not be permitted to enter the facility and the Screener will verbally direct the individual to the COVID-19 Body Temperature Screening Program Notice (Attachment I) and to contact his or her supervisor or employer (as applicable) for further instructions. If the individual is a member of the public, the Screener will direct the individual to the COVID-19 Body Temperature Screening Program Notice (Attachment I) only.

Body Temperature Measuring Devices:

- Infrared thermometers measures skin temperatures from 89.6 to 108.5˚F (32.0 to 42.5˚C) at a distance of at least 1 inch to alleviate the need to contact the individual. Infrared light performs in the same manner as visible light. It can be focused, reflected, or absorbed. Infrared thermometers uses its lens to focus infrared light from one object onto a detector

in the device called a thermopile. The thermopile absorbs the infrared radiation and turns it into heat. The more infrared energy, the hotter the thermopile. This heat is turned into electricity. The electricity is sent to a detector, which uses it to determine the temperature of the individual. The thermometers will alarm visually (and audibly if enabled) when it reads a temperature of 100.4˚F or above. The memory within the thermometer has the ability to store up to 32 individual temperature readings. The oldest image will be overwritten and discarded as the thermometer reaches 32 images.

- Thermographic imaging cameras provides video images of human body temperatures (typically the tear-duct/eye area) at a distance of approximately 10 feet. This area of the face emits heat that provides the closest reading of a body temperature. This camera will measure temperature levels of 89.6 to 108.5˚F (32.0 to 42.5˚C). The devices monitor and detect significant rises in skin surface temperatures, which is typically associated with an individual having an elevated body temperature. Thermographic imaging cameras distinguish the relative temperature of surrounding objects to help the Screener see warmer objects, such as people or animals, against cooler backdrops. Individuals scanned by thermographic imaging cameras appear as yellow-to-red glowing entities that are not personally identifiable. BEP's Thermographic Imaging Cameras will include hand-held models or those that can be mounted on a tripod. The mounted version provides a computer interface (including Wi-Fi capabilities) and software used to configure settings and enhance image quality. If interfaced to the network, the devices can stream images continuously. The handheld cameras provide connectivity via Universal Serial Bus (USB) and a removable storage device capable of storing 8 Gigabytes (GB) of information.

To protect the privacy of individuals impacted by this Program, BEP will only permit Screeners to track the following statistical data for reporting purposes:

- Number of individuals screened;
- Number of individuals denied access;
- Number of individuals granted access; and
- Average wait times.

BEP will further mitigate the Program's privacy risks through the following activities**:**

- Screeners may use Portable Privacy Partitions/Screens when measuring body temperatures other than when occupant(s) remain in the vehicle to protect the privacy and confidentiality of the individual during the body temperature screening.

- As with all medical information, Screeners shall keep the fact that an individual has an elevated temperature and the elevated temperature confidential. Screeners shall direct individuals attempting to enter the facility to maintain a distance of 10 feet or more (as needed) between each person awaiting screening to reduce the risk of any unauthorized information disclosure or communications being overheard by others present in the collection site.

- Should screening procedures change due to inclement weather, Screeners shall maintain the same privacy and confidentiality protections.

- Screeners shall not request information and/or ask questions related to the elevated temperature, COVID-19 symptoms or information pertaining to the individual.

- After collecting/taking and displaying or communicating verbally (in a low-pitched/ discreet voice) the body temperature to the individual, Screeners shall not record any information such as name, body temperature, signs of flushed cheeks or fatigue, coughing or shortness of breath, or any other identifying information.

- For the visually impaired, or when the elevated temperature is delivered verbally, the Screener will communicate the information in a low pitched voice and discreetly so that no one other than the individual becomes aware of the elevated temperature.

- Although the infrared thermometers can provide the body temperatures in audio format, the Screeners are required to disable the audible alarm if the thermometer has an alarm function to sound when a temperature reading rises above a programmable set point. BEP will also disable any audible alarms on thermographic imaging cameras or associated software.

- The BEP designated non-invasive/non-contact/no-touch infrared thermometers or thermographic imaging cameras shall not record/store the body temperature in any format. BEP Chief Information Technology Directorate (CIO) will use a stand-alone server to support this technology to mitigate network connectivity or provide a means for co-mingling any data with existing BEP systems or information. The CIO will not configure its thermographic imaging cameras software or USB to stream images continuously or retain images or body temperature readings. Audible alarms on all devices will be disabled.

- BEP will use the thermographic imaging camera software to enhance the image's focus, color variations, distance from objects, processing capabilities, disable audible alarms, and to operate maintenance features. It will not be used to store, access, move, or edit video files. BEP will also refrain from creating routes to download data for purposes other than to direct images to applicable viewing monitors, when needed. BEP will also prevent Screeners from accessing features or settings that are not related to measuring body temperature ranges and viewing the resulting image.

- BEP supervisors will store BEP employee's medical-related records, if needed, separate from BEP employee personnel records.

- BEP further mitigates privacy, civil rights and liberties, and cyber security concerns by requiring all employees and contractors to take annual Privacy Awareness Training, titled: A Culture of Privacy Awareness, and Cybersecurity Awareness Training.

The internal Standard Operating Procedure (SOP) of the COVID-19 Body Temperature Screening Program include facility-specific screening protocols pertaining to screening site locations, screening hours, and staffing levels.

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: 5 U.S.C. § 301,[1] 31 U.S.C. § 303,[2] 31 U.S.C. 321,[3]44 U.S.C. § 3534[4], and 29 CFR Part 1630[5].

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 conditions 5 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?

---

[1] 5 U.S.C. § 301.
[2] 31 U.S.C. § 303.
[3] 31 U.S.C. § 321.
[4] 44 U.S.C. § 3534.
[5] 29 CFR Part 1630.

BEP uses the Privacy Threshold Analysis (PTA) process to assess and limit PII collection to information that is deemed relevant and necessary in order to conduct authorized business activities. BEP also provides a continuous monitoring framework that triggers additional PTA updates each time the system or processes impacting PII are significantly altered.

An assessment of the Body Temperature Screening Program determined that the body temperature reading constitutes PII. Although the body temperature reading and the fact that the individual has an elevated temperature is considered medical information and PII, the Screeners will not retain the PII (body temperature reading) in any form after conducting the screening. Additionally, infrared thermometers and thermographic imaging cameras will not retain videos/images or body temperature numbers. During the screening process, the body temperature readings (PII/biometric data literally from the individual's body) will not be associated with the name, or an identifying number, symbol or other identifying particular assigned to the individual undergoing screening. Therefore, the collection of this information does not meet the parameters of a "record" in accordance with the Privacy Act of 1974, 5 U.S.C. 552a(4) at the moment of temperature collection. However, BEP employees providing medical information and/or time and attendance information, as described in Section 4.2 below, to his or her supervisor through communications following the denied entry into a BEP facility, may become part of an existing Privacy Act System of Records. As described in Section 6.1 below, the following SORNs apply to BEP employees: Privacy Act records: OPM/GOVT-10 - Employee Medical File System Records - 75 FR 35099 (June 21, 2010), and Treasury .001 - Treasury Payroll and Personnel System - 81 FR 78266 (Nov. 7, 2016). In order to manage the accounts of Screeners authorized to use Thermographic Imaging Camera systems, BEP will collect user account and system access PII (e.g. user names, passwords, computer name, and IP Addresses) under the auspices of Treasury .015 - General Information Technology Access Account Records - 81 FR 78266 (Nov. 7, 2016).

Additionally, BEP incorporates a Risk Management Framework assessment into its PTAs to evaluate and categorize the PII confidentiality impact level (e.g. low, moderate, or high) to indicate the potential harm to individuals and/or the organization if PII were inappropriately accessed, used, or disclosed. By eliminating the need to retain the temperature readings at the time of collection, BEP minimizes the risk of collecting PII that is not relevant and necessary.

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 Mailing Address and Office Name	☒ Business Cell Number	☒ Business Phone or Fax Number
☒ 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): Tested Individual's Job Title
☒ Other (please describe): Office title and location	☒ Other (please describe): Time and Attendance Information (work status and leave data)	☐ 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): COVID-19-related diagnoses/prognosis from physicians/medical personnel.		

Biometrics/Distinguishing Features/Characteristics of Individuals		
☐ Physical description/ characteristics (e.g., hair, eye color, weight, height, sex, gender etc.)	☐ Signatures (including digital)	☐ 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): Body Temperature Reading	☐ 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. Time and Attendance information (work status and leave data)
☐ 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): Metadata/user access statistical data.	☐ Other (please describe): Access group name.	☐ Other (please describe): _____

Other	
☒ Other (please describe): Statistical Information for the program consists of:	☐ Other (please describe: _____

Non-PII: • Number of individuals screened; • Number of individuals denied access; • Number of individuals granted access; and • Average wait times.	
☐ Other (please describe: _____	☐ Other (please describe: _____

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

BEP Employee	BEP Contractor	Members of the Public, including non BEP Federal government employees and contractors
Specific PII identified in Section 4.2 acquired from this source: **Collected at DCF/WCF Entrances:** • Body Temperature Reading **Collected by Supervisors after a denied entry:** • Name • Date of Birth • Full and/or Truncated Social Security Number (SSN) • Employee ID Number • Medical Information, which may include COVID-19-related diagnoses/prognosis statements from physicians/medical personnel. • Home and Business Address • Personal and Business Email Address • Personal and Business Telephone Number • Time and Attendance Data **Collected by CIO IT Administrators to Manage Access to Thermographic Imaging Camera Technology and Associated Information System:** • Office title and location • Office/work telephone number • User Name/Login • Password • IP Address • Computer name • Access Group Name	**Specific PII identified in Section 4.2 acquired from this source:** • Body Temperature Reading	**Specific PII identified in Section 4.2 acquired from this source:** • Body Temperature Reading

• Metadata/User Access Statistical Information		
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): N/A	Please identify the form name (or description) and/or number (e.g., OMB Control Number): N/A	Please identify the form name (or description) and/or number (e.g., OMB Control Number): N/A
☒ 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 (No credit card information)	☐ 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): Infrared Thermometers or Thermographic Imaging Cameras (without data retention)	☒ Extracted from particular technology (e.g., radio frequency identification data (RFID) devices, video or photographic cameras, biometric collection devices): Infrared Thermometers or Thermographic Imaging Cameras (without data retention)	☒ Extracted from particular technology (e.g., radio frequency identification data (RFID) devices, video or photographic cameras, biometric collection devices): Infrared Thermometers or Thermographic Imaging Cameras (without data retention)
☐ 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: HR/Time and Attendance Databases/Systems	☐ Other: Please describe:	☐ Other: Please describe:
☒ Other: Please describe:	☐ Other: Please describe:	☐ Other: Please describe:

Network interface	_____	_____

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.

Although Screeners will not retain any information, including the body temperature reading, all individuals subject to body temperature screening are provided highly visible notice at the collection site. (Attachment I) Individuals denied entry will receive an additional notice with specific medical guidance (Attachment II). BEP Employees that are denied entry will receive medical and personnel guidance and the required Privacy Act Statement as described in Section 4.4(c) above.

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. Therefore, and in an effort to reduce risk to individuals and federal agencies, OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, (May 22, 2007) required agencies to reduce the use of SSNs in agency systems and programs and to identify instances in which the collection is superfluous. In addition, OMB mandated agencies to explore alternatives to agency use of SSNs as personal identifiers for Federal employees and members of the public.

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. *If checked, please provide the name of the system of records in the space provided below:*

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.

BEP will limit PII collection for individuals attempting to enter BEP facilities to the body temperature reading. BEP Employees may provide their full or truncated SSN or Employee ID Number associated with medical and/or time and attendance (work status and leave data) processing within BEP Human Resources databases or systems. There is no SSN impact to BEP Contractors or members of the public.

First Amendment Activities

The Privacy Act provides 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(b)(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(i) 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.

☐ N/A, the system or project does not maintain any information describing how any individual exercises their rights guaranteed by the First Amendment.

N/A.

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.

BEP Screeners within the Office of Environmental Health and Safety and WCF Police Officers of the Office of Manufacturing Support Western Currency Facility, Security Division will use PII (the "biometric" body temperature reading) to permit or deny entry into BEP facilities in order to protect all individuals within BEP against the spread of the COVID-19.

BEP managers and supervisors may use additional PII (medical and time and attendance information) provided by BEP employees to their supervisor to document and/or manage personnel-related matters under the auspices of Privacy Act System of Records Notice OPM/GOVT-10 - Employee Medical File System Records - 75 FR 35099 (June 21, 2010) and Treasury .001 - Treasury Payroll and Personnel System - 81 FR 78266 (Nov. 7, 2016).

BEP CIO IT Administrators may use additional PII (system account access and management information as described in Section 4.2 and 4.3 above) to grant access and manage accounts for BEP Screeners within the Office of Environmental Health and Safety and WCF Police Officers of the Security Division under the auspices of Treasury .015 - General Information Technology Access Account Records - 81 FR 78266 (Nov. 7, 2016).

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?
See Section 5.2(f) below.

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?
N/A.

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?
There are no exemptions claimed for the following System of Records Notices: OPM/GOVT-10 - Employee Medical File System Records - 75 FR 35099 (June 21, 2010); Treasury .001 - Treasury Payroll and Personnel System - 81 FR 78266 (Nov. 7, 2016); and Treasury .015 - General Information Technology Access Account Records - 81 FR 78266 (Nov. 7, 2016).

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?
N/A.

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?
BEP collects body temperature readings directly from the subject individual seeking access to a BEP facility. If an individual registers a body temperature at or above 100.4˚F, they will experience the adverse action of being denied access to a BEP facility. BEP minimizes any potential risks regarding accuracy, relevance, timeliness, and completeness of records by not retaining the body temperature reading in any form. Screeners are only able to retain (1) number of individual screened, (2) number of individuals denied access, (3) number of individuals granted access, and (4) average wait times. BEP employees maintain the ability to review and correct any additional medical information that they provide to their supervisor. Collecting minimal PII (the body temperature reading) and not associating it with an individual or storing the information at the screening level further minimizes BEP's risk of sharing inaccurate information that could be used to make determinations about an individual.

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?

Screeners do not retain the body temperature reading in any form. There is no additional information used or merged with body temperature reading collected from individuals attempting to enter a BEP facility. The COVID-19 Body Temperature Program SOP specifically prohibits data retention or merging information (including medical information) pertaining to COVID-19 with an employee's existing medical or personnel records. Body temperature readings taken at the time of attempted entry into a BEP facility that measure at or above 100.4˚F will result in a determination that an individual will not be granted access to a BEP facility.

BEP supervisors may merge time and attendance information (work status and leave information) pertaining to BEP employees that are denied entry to a BEP facility with existing human resources systems and databases used to process leave requests. The COVID-19 Body Temperature Program SOP specifically prohibits BEP supervisors merging records pertaining to COVID-19 with existing personnel records.

Collecting minimal PII for BEP uses further minimizes BEP's risk of sharing inaccurate information that could be used to make additional determinations about an individual. BEP deems accurate any medical or time and attendance information provided by BEP employees to their supervisor following a denied entry.

BEP minimizes potential risks regarding accuracy, relevance, timeliness, and completeness or records by collecting the information directly from the BEP employee. The employee maintains the ability to review and correct their information at the time of initial or subsequent submission. Collecting minimal PII for BEP uses further minimizes BEP's risk of sharing inaccurate information that could be used to make determinations about an individual.

BEP does not retain information of any kind pertaining to contractors or members of the public, including non-BEP Federal government employees and contractors.

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)?

BEP uses the PTA review process to access systems, applications, and information collection initiatives to ensure data accuracy, completeness, and timeliness for all programs, initiatives, and IT systems. This assessment becomes part of the Federal Information Security Modernization Act (FISMA) annual review process.

BEP issued a Body Temperature Screening Program Standing Operating Procedures (SOP) document to ensure that Screeners follow strict privacy protocols and processes. These protocols and procedures restrict information collection to the body temperature reading, without further retention of information in an identifiable form. Any additional medical information provided by a BEP employee that was denied entry to their supervisor will be provided directly by the employee and stored separately from existing personnel records. BEP employees will continue to follow existing Human Resources policies and procedures for processing personal leave requests when needed. Collecting information directly from BEP employees will ensure information accuracy, completeness, and timeliness.

The BEP designated non-invasive/non-contact/no-touch infrared thermometers or thermographic imaging cameras will not record/store the body temperature in any format. The infrared thermometers may store up to 32 individual temperature readings but the oldest image will be overwritten and discarded as the thermometer reaches the 32 image threshold. BEP Chief Information Technology Directorate (CIO) will use a stand-alone server to support this technology to mitigate network connectivity or provide a means for co-mingling any data with existing BEP systems or information. CIO IT Administrators will not configure its thermographic imaging cameras software or USB to stream images continuously or retain images or body temperature readings. Audible alarms on all devices will be disabled.

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

Section 5.2(n) ☐ Yes ☒ No 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?

Since BEP collects the body temperature reading directly from the individual to whom it pertains, BEP deems this information accurate. BEP employees reserve the right to correct any additional information provided to their supervisor if they are denied entry due to an elevated body temperature by submitting a Privacy Act request.

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 body temperature reading collected from the individual at the time of attempted entry are not retained or stored in any form. Any additional medical information provided by BEP employees to their supervisor will be stored separately and used to document and/or manage medical-related matters under the auspices of Privacy Act System of Records Notice OPM/GOVT-10 - Employee Medical File System Records - 75 FR 35099 (June 21, 2010). User account and system access PII (e.g. user names, passwords, computer name, and IP Addresses) will be managed under the auspices of Treasury .015 - General Information Technology Access Account Records - 81 FR 78266 (Nov. 7, 2016). BEP will not alter such information arbitrarily unless directed to do so by the individual through a Privacy Act request.

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 ☐ N/A 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")?

BEP does not retain the body temperature reading. Therefore, it is not possible to associate a particular reading with an individual or share any information pertaining to a particular individuals with third parties within the Department of the Treasury. Screeners are only permitted to share/display the temperature reading to the individual undergoing screening only.

BEP supervisors may share medical and time and attendance information pertaining to BEP employees that were denied entry into a BEP facility with Department of the Treasury personnel who have a need to know in the performance of their official duties.

BEP does not collect or disseminate information on BEP contractors or members of the public, including non BEP Federal Government employees and contractors.

Screeners are permitted to share non-PII statistical information stated in Section 4.2 above with COVID-19 Body Temperature Screening Program Managers or individuals within the Department of the Treasury that have a need to know the information in the performance of official duties.

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 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?

N/A.

Internal Information Sharing Chart

Internal Recipient's Name (e.g., bureau or office)	Office of Environment, Health, ad Safety (OEHS)	Office of Human Resources (OHR)	CIO IT Administrators
Purpose of the Sharing	To manage medical records and documentation pertaining to BEP employees, and to manage the COVID-19 Temperature Screening Program.	To manage time and attendance transactions and records for BEP employees that are required to take leave following a denied entry due to an elevated body temperature.	To manage Thermographic Imaging Camera user accounts, and to perform auditing and compliance activities.
PII Shared	• Name • Date of Birth • Full and/or Truncated Social Security Number (SSN) • Employee ID Number • Medical Information, which may include COVID-19-related diagnoses/prognosis statements from physicians/medical personnel. • Home and Business Address • Personal and Business Email Address • Personal and Business Telephone Number	• Name • Date of Birth • Full and/or Truncated Social Security Number (SSN) • Employee ID Number • Time and Attendance Data • Home and Business Address • Personal and Business Email Address • Personal and Business Telephone Number	• User Name/Login • Password • IP Address • Computer Name • Access Group Name • Metadata/User Access Statistical Information

Applicable Statutory or Regulatory Restrictions on Information Shared	N/A	N/A	N/A
Applicable Restrictions Imposed by Agreement on Information Shared (e.g., by Treasury agreement with the party that provided the information to Treasury)	N/A	N/A	N/A
Name and Description of MOU or Other Agreement Restricting Treasury's Internal Use, Maintenance, Handling, or Sharing of PII Received	N/A	N/A	N/A
Method of PII Transfer (e.g., paper/oral disclosures/magnetic disk/portable device/email/fax/other (please describe if other)	• Paper • Email • Oral disclosures	• Secure electronic transmission • Paper • Email • Oral disclosures	• Network interface • System access network portals
Screeners does not retain or share body temperature readings. Screeners will share non-PII statistical information as described in Section 4.2 above with Senior BEP Managers that need the information in the performance of official duties and to provide oversite of the BEP COVID-19 Temperature Screening Program.			

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?
BEP does not retain body temperature readings but may share information externally in accordance with the Routine Uses in applicable Privacy Act System of Records Notices listed in Section 6.1 below.

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?

Screeners do not retain the body temperature reading or create records that require accounting of disclosures. BEP accounts for disclosures of medical or time and attendance information provided by BEP employees to their supervisor following a denied entry will be processed under the auspices of Privacy Act System of Records Notice OPM-GOVT-10 - Employee Medical File System Records - 75 FR 35099 (June 21, 2010) and Treasury .001 - Treasury Payroll and Personnel System - 81 FR 78266 (Nov. 7, 2016). Accounting and disclosures of user account and system access PII (e.g. user names, passwords, computer name, and IP Addresses) will be managed under the auspices of Treasury .015 - General Information Technology Access Account Records - 81 FR 78266 (Nov. 7, 2016).

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)?

N/A.

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?

N/A.

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?

There are no agreements with entities outside of the Department of the Treasury.

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?

N/A.

External Information Sharing Chart

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

External Recipient's Name	Federal, State, or local agency personnel.	Appropriate agencies, entities, and persons.
System/Application	Coronavirus Disease 19 (COVID-19) Body Temperature Screening Program	Treasury .015 – General Access and Account Records
Purpose of the Sharing	To the extent necessary to comply with laws governing reporting of communicable disease.	To provide information externally in response to the suspected pertaining to individuals who provide personal information in order to facilitate access to Treasury information technology resources.
PII Shared	• Name • Date of Birth • Full and/or Truncated Social Security Number (SSN) • Employee ID Number • Medical Information, which may include COVID-19-related diagnoses/prognosis statements from physicians/medical personnel. • Home and Business Address • Personal and Business Email Address • Personal and Business Telephone Number • Time and Attendance Data	• Office title and location • Office/work telephone number • User Name/Login • Password • IP Address • Computer name • Access Group Name • Metadata/User Access Statistical Information
Content of Applicable Routine Use/Citation to the SORN	To disclose to a requesting agency, organization, or individual the home address and other information concerning those individuals who it is reasonably believed might have contracted an illness or been exposed to or suffered from a health hazard while employed in the Federal workforce. OPM/GOVT-10 - Employee Medical File System Records	To appropriate agencies, entities, and persons when Treasury suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; or as is reasonably necessary to assist in connection with Treasury's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm. Treasury .015 – General Access and Account Records
Applicable Statutory or Regulatory or Restrictions on Information Shared	N/A	N/A

Name and Description of Relevant MOUs or Other Agreements Containing Sharing Restrictions Imposed on Treasury by an External Source or Source/Originating Agency (including description of restrictions imposed on use, maintenance, and disclosure of PII)	N/A	N/A
Name and Description of Relevant MOUs or Other Agreements Containing Restrictions Imposed by Treasury on External Sharing Partner (including description of restrictions imposed on use, maintenance, and disclosure of PII)	N/A	N/A
Method(s) Used to Transfer PII (e.g., paper/ oral disclosures/magnetic disk/portable device/email fax/other (please describe if other)	• Electronically • Email • Fax • Telephonically • Orally	• Electronically • Email • Magnetic disk • Portable device
Screeners do not retain or share body temperature readings externally. Medical information provided by BEP employees to their supervisor following a denied entry will be managed within the Department of the Treasury and only shared under the auspices of Privacy Act System of Records Notice OPM-GOVT-10 - Employee Medical File System Records - 75 FR 35099 (June 21, 2010). User account and system access PII (e.g. user names, passwords, computer name, and IP Addresses) will be shared under the auspices of Treasury .015 - General Information Technology Access Account Records - 81 FR 78266 (Nov. 7, 2016).		

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))?
No additional comments.

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?
Screeners do not retain the body temperature reading or retrieve information by a personal identifier. Medical information provided by BEP employees to their supervisor following a denied entry will be shared under the auspices of Privacy Act System of Records Notice OPM-GOVT-10 - Employee Medical File System Records - 75 FR 35099 (June 21, 2010) and retrieved by name and date of birth. BEP will not collect any information from BEP Contractors or members of the public other than measuring body temperature prior to entering the facility. Time and Attendance information provided by BEP employees under Treasury .001 - Treasury Payroll and Personnel System - 81 FR 78266 (Nov. 7, 2016) is accessed by name. User account and system access PII (e.g. user names, passwords, computer name, and IP Addresses) will be managed under the auspices of Treasury .015 - General Information Technology Access Account Records - 81 FR 78266 (Nov. 7, 2016) and retrieved by name, IP Address, or Computer Name.

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 program does not maintain the collected body temperature readings in an identifiable form. There are no information requests or assigned OMB Control Numbers for this program.

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 destroyed 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 ☐ N/A 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 2.2: Employee Management Records

  Item 080 - DAA-GRS-2017-0007-0012 - Supervisor's Personnel Files.
  Records on positions, authorizations, pending actions, position descriptions, training records, individual development plans, telework agreements, award recommendations, and records on individual employees not duplicated in or not appropriate for the OPF. These records are sometimes called supervisors' working files, unofficial personnel files (UPFs), and employee work folders or "drop" files.

  Exclusion 1: Records that become part of a grievance file, an appeal or discrimination complaint file, a performance-based reduction-in-grade or removal action, or an adverse action. These records are covered under GRS 2.3, Employee Relations Records.

  Exclusion 2: Employee medical documents, unless part of employee's initial request for reasonable accommodation. Following approval, the agency's reasonable accommodation decision replaces medical documentation and becomes the record. Reasonable accommodation employee case files are covered under

- GRS 2.4: Employee Compensation and Benefits Records

  Item 030 – DAA-GRS-2019-0004-0002 - Time and attendance records.
  Sign-in/sign-out records, time cards, leave applications and approvals of all types (annual, sick, family medical, military service, jury duty, leave donations, etc.); overtime, compensatory, and credit time requests and approvals; premium pay authorizations; and other records documenting employees' presence at or absence from work. Temporary. Destroy when 3 years old, but longer retention is authorized if required for business use.

  GRS 3.2. Information Systems Security Records

  Item 030 – DAA-GRS-2013-0006-0004 – System Access Records
  These records are created as part of the user identification and authorization process to gain access to systems. Records are used to monitor inappropriate systems access by users. Includes records such as:

- User profiles
- Log-in files
- Password files
- Audit trail files and extracts
- System usage files
- Cost-back files used to assess charges for system use

Exclusion 1. Excludes records relating to electronic signatures.

Exclusion 2. Does not include monitoring for agency mission activities such as law enforcement.

Systems not requiring special accountability for access. DAA-GRS-2013-0006-0003 - These are user identification records generated according to preset requirements, typically system generated. A system may, for example, prompt users for new passwords every 90 days for all users. Temporary. Destroy when business use ceases.

Systems requiring special accountability for access. These are user identification records associated with systems which are highly sensitive and potentially vulnerable. DAA-GRS-2013-0006-0004. Temporary. Destroy 6 years after password is altered or user account is terminated, but longer retention is authorized if required for business use.

SORN Record Schedules:

- OPM/GOVT-10 – Employee Medical File System Records are maintained for the period of the employee's service in the agency and is then transferred to the National Personnel Records Center for storage, or as appropriate, to the next employing Federal agency. Other medical records are either retained at the agency for various lengths of time in accordance with the National Archives and Records Administration's records schedules or destroyed when they have served their purpose or when the employee leaves the agency. Within 90 days after the individual separates from the Federal service, the EMF is sent to the National Personnel Records Center for storage. Destruction of the EMF is in accordance with General Records Schedule-1(21). Records arising in connection with employee drug testing under Executive Order 12564 are generally retained for up to 3 years. Records are destroyed by shredding, burning, or by erasing the disk.

- Treasury .001 - Treasury Payroll and Personnel System Records and the current payroll and personnel system and the personnel and payroll system's master files are kept as electronic media. Information rendered to hard copy in the form of reports and payroll information documentation is also retained in an electronic media format. Employee records are retained in automated form for as long as the employee is active on the system (separated employee records are maintained in an "inactive" status). Files are purged in accordance with Treasury Directive 80-05, "Records and Information Management Program."

- Treasury .015, General Information Technology Access and Accounts Records are maintained in accordance with the National Archives and Records Administration's General Records Schedule 24, section 6, ''User Identification, Profiles, Authorizations, and Password Files.'' Inactive records will be destroyed or deleted 6 years after the user account is terminated or password is altered, or when no longer needed for investigative or security purposes, whichever is later.

Screeners do not retain body temperature readings following collection and display. BEP employees may create medical and time and attendance records and provide such information to their supervisor following a denied entry. BEP may also generate policies, procedures, and/or statistical records pertaining to the COVID-19 Body Temperature Screening program. BEP will collect user account and system access PII during the process of granting access to BEP employees and contractors that have a need to operate and/or manage Thermographic Imaging Camera support systems.

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?
The Infrared Thermometers and the Thermographic Imaging Cameras do not constitute a FISMA-regulated system based on its lack of data retention, use parameters, storage prohibitions, and hardware/software configuration. Should this posture change, BEP will reassess the FISMA compliance posture and information security categorizations.
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?
BEP assigns personnel to specific groups within its Active Directory, which serves as a tool for granting role-based access. In addition, BEP uses its Identity and Access Management System (IDM) to process access requests and conduct identity verification and authentication. Groups within the Active Director range from normal users to OEHS System Administrators. OEHS System administrators provide additional access controls within the thermographic imaging camera application by authorizing and assigning Screeners as "users." BEP limits access to the application Screeners from the DCF Office of Environmental Health and Safety (OEHS) and WCF Police Officers of the Security Division, who operate the system in the performance of their official duties.
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)?
BEP reduces its security and privacy risks by collecting the body temperature reading directly from the individual attempting to enter a BEP facility or from BEP Employees that provide medical information to their supervisor subsequent to a denied entry. BEP further reduces security and privacy risks by not collecting additional data or retaining the body temperature readings after collecting and displaying the information to the individual. Security and Privacy risks for Thermographic Imaging Camera support systems are mitigated by limiting access to BEP personnel within the DCF Office of Environmental Health and Safety (OEHS) and WCF Police Officers of the Security Division, who maintain a need to access the system for official purposes.
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?
BEP will not retain information from Infrared Thermometers or Thermographic Imaging Cameras. Statistical information obtained as described in Section 4.2 above will be captured by Screeners manually. Prior to granting access to Thermographic Imaging Camera support systems, BEP will determine if the user has a need to access the system in the performance of official duties. BEP assigns employees and contractors to specific groups within its Active Directory, which serves as a tool for granting role-based access. In addition, BEP uses its Identity and Access Management System (IDM) to process access requests and conduct identity verification and authentication. Groups within the Active Director range from normal users to system administrators.
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?

N/A.

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?
The BEP CIO Directorate conducts periodical audits of all IT systems in order to monitor user activity and to ensure that data is not exposed to unauthorized individuals. OEHS System Administrators also create and manage all accounts and use parameters.

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 and/or employ various 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?
The Body Temperature Screening Program or any of its technologies is not accessible by members of the public and is restricted to the BEP workforce designated in Section 6.4c above. BEP performs a continuous review in order to (1) determine the user community authorized to operate the Thermographic Imaging Camera application, (2) employ various accessibility features into its software products, and (3) to procure specific tools for personnel use in compliance with Section 508 of the Rehabilitation Act, as amended in 1998. Should a disabled employee require access to information from the system, BEP will provide the information to the employee in an appropriate and preferred format for the individual.

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 and Privacy Act?
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?
These parameters apply to the applicable SORNs associated with the COVID-19 Body Temperature Screening Program: OPM/GOVT-10 Employee Medical File System Records - 75 FR 35099 (June 21, 2010; Treasury .001 - Treasury Payroll and Personnel System - 81 FR 78266 (Nov. 7, 2016); and Treasury .015 - General Information Technology Access Account Records - 81 FR 78266 (Nov. 7, 2016).

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)?
BEP employees submit their own medical information to their supervisor subsequent to a denied entry. They may correct their information at the time of initial or subsequent submission in addition to pursuing redress through the Privacy Act and FOIA processes. BEP employees may change or correct their information at their discretion within BEP, Treasury, or federal human resources databases.

Responsible Officials

Bureau Privacy Official
Anthony Johnson
Government Information Specialist (Privacy)
Office of Critical Infrastructure and IT Security
Bureau of Engraving and Printing
Department of the Treasury

Reviewing Official
Togai Andrews
Chief, Office of Critical Infrastructure and IT Security
Bureau of Engraving and Printing
Department of the Treasury

Approval Signature

//S// 10/28/2020

_____
Togai Andrews
Office of Critical Infrastructure and IT Security

ATTACHMENT I

COVID-19 BODY TEMPERATURE SCREENING PROGRAM NOTICE

In accordance with the Centers for Disease Control and Prevention (CDC) Guidance, which is aimed at the prevention of introducing COVID-19 to the workplace, the BEP is measuring body temperatures of individuals prior to granting access to this facility. If the screening process shows that you have an elevated temperature, which is at or above 100.4˚F, you will not be granted access to this facility. Written notification regarding the appropriate next steps will be provided by the screening personnel. If you refuse to participate in the screening process, you will not be granted access to this facility. Because your body temperature will not be recorded in any format, you will be re-screened each time you seek access to the facility. However, if you exist the facility and return the same day, you may receive a re-entry card before existing the facility. Thank you in advance for your cooperation. Stay safe and healthy.

ATTACHMENT II

COVID-19 ELEVATED TEMPERATURE SCREENING NOTICE TO INDIVIDUALS

Members of the Public, including Non-BEP Federal employees and contractors:
Because you have an elevated temperature, which is at or above 100.4˚F, you have been denied access to this BEP facility. You are instructed to depart the area immediately and follow the Centers for Disease Control and Prevention (CDC) recommended steps and precautions. Because BEP will not record your elevated temperature in any format, you will be re-screened each time you seek access to this BEP facility. Thank you.

BEP Employees:

Because you have an elevated temperature, which is at or above 100.4˚F, you have been denied access to this BEP facility. You are instructed to depart the area and inform your supervisor within 60 minutes after receiving this notice that you have been denied entry to the facility. The type of leave to be used and a return to work determination will be conducted on an individual basis. The Screener will not record your elevated temperature in any format.

While at home, you should monitor symptoms and, if they worsen, consult a doctor or use a tele-medicine type service. You must maintain contact with your supervisor and keep your supervisor informed of your condition. Your supervisor will store any medical-related records, if needed, separate from your personnel records, and in accordance with the Office of Personnel Management Privacy Act System of Records Notice (OPM/GOVT-10) Employee Medical File System Records - 75 FR 35099 (June 21, 2010.) Your information will only be shared with individuals that have a need- to- know in the performance of official duties and in accordance with OPM and/or other applicable Privacy Act System of Records Notice.

If you refused to be screened, you must notify your supervisor immediately and report that you refused to be screened. Refusal to screen may result in disciplinary action. The Screener will not record your refusal.

BEP Contractors:

Because you have an elevated temperature, which is at or above 100.4˚F, you have been denied access to this BEP facility. At this time, we ask that you depart the area and inform your employer that you have been denied access. BEP will not record your elevated temperature in any format. Your employer will provide you with additional guidance regarding this matter. Please do NOT disclose to BEP, including to the Contracting Officer or the Contracting Officer Representative, your medical information such as whether you have an elevated temperature or COVID-19 diagnosis.