BUREAU OF ENGRAVING AND PRINTING
CIRCULAR

No. 25-01.1

DATE January 27, 2020

PRIVACY AND CIVIL LIBERTIES POLICIES, COMPLIANCE AND RESPONSIBILITIES, AND SAFEGUARDING OF PERSONALLY IDENTIFIABLE INFORMATION (PII)

REVIEW DATE: January 27, 2025

1.0 PURPOSE AND SCOPE

This circular establishes the Bureau of Engraving and Printing's (BEP/Bureau) policies, compliance requirements, and responsibilities concerning privacy and civil liberties. In addition, this circular provides guidance on how to safeguard Personally Identifiable Information (PII).

This circular applies to BEP employees and contractors when engaged or handling information, programs, activities, social media, information systems, information technologies, or operations that impact the privacy of individuals.

2.0 POLICY

2.1 It is the policy of the BEP to evaluate information collection activities, programs, systems, and operations to identify privacy risks and mitigation strategies to reduce potential privacy impacts. BEP is required to:

2.1.1 Perform a Privacy Threshold Analysis (PTA) when a new system development is initiated, or an enhancement or modification is undertaken on an existing system to determine if PII is present and is either from or about the public.

2.1.2 Conduct a Privacy and Civil Liberties Impact Assessment (PCLIA) before developing or procuring information technology (IT) systems or projects that collect, maintain, or disseminate information that is in an identifiable form from or about members of the public. Conduct and update PCLIAs as necessary where an IT system change creates new privacy risks. Conduct a PCLIA when issuing new or updated rulemaking that affects personal information and when initiating, consistent with the Paperwork Reduction Act, a new electronic collection of information in identifiable form for ten or more persons (excluding agencies, instrumentalities, or employees of the federal government).

2.1.3 Make PCLIAs publicly available on the Bureau public website, in the Federal Register, or by some other means.

2.1.4 Post privacy policies on agency websites used by the public.

2.1.5 Provide appropriate information security that protects BEP information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction to protect personal privacy.

2.1.6 Use data security measures (e.g., BEP's secure messaging system, encryption, or password protection) to securely transmit all emails that contain PII outside of the Treasury/BEP Network.[1]

2.1.7 Report annually to the Office of Management and Budget (OMB) on compliance with Section 208 of the E-Government Act of 2002.

2.1.8 Conduct periodic reviews of PII holdings to ensure that these holdings are accurate, relevant, timely and complete, and reduce their holdings of PII to the minimum necessary to effectively administer Bureau programs.

2.1.9 Periodically review and update policies, guidance, and procedures that address the manner in which occurrences of breaches of PII can be prevented and their effects minimized.

2.1.10 Report all suspected or confirmed privacy incidents involving PII to the Computer Security Incident Response Center (CSIRC) within one business day after it is reported to the Bureau IT Service Desk. Ensure all employees and contractors report all suspected or confirmed privacy incidents within one hour of discovery.

2.1.11 Provide annual privacy training to employees who have access to PII. Such training shall instruct such individuals of their responsibility to appropriately safeguard PII and the disciplinary and legal consequences of not doing so.

2.1.12 Establish internal procedures consistent with Section 803 of the Implementing Recommendations of the 9/11 Commission Act of 2007 and this directive to ensure that the Bureau appropriately considers privacy and civil liberties in program development and implementation.

2.1.13 Ensure that accurate and complete written reporting information that meets the requirements of Section 803 and this circular are submitted in a timely manner to the Chief Privacy and Civil Liberties Officer for reporting purposes.

2.1.14 Ensure that the Bureau has adequate procedures to receive, investigate, respond to, and redress complaints from individuals who allege violation of their privacy or civil liberties, and adequate procedures to protect against reprisals or threats of reprisals against employees who make a complaint or disclose information that indicates a possible violation of privacy protections or civil liberties in the Bureau's administration of programs and operations.

2.1.15 Establish, implement, and ensure compliance with policies, procedures, and standards necessary to comply with the Information Sharing Environment (ISE) Privacy Guidelines.

2.1.16 Identify paper record collections and electronic information systems that contain protected information and ensure that the names of these collections and systems are provided to the Treasury Deputy Assistant Secretary for Privacy, Transparency, and Records (DASPTR).

[1] BEP Standing Operating Procedure (SOP), Sending Secure Email form BEP, May 8, 2017, *Available at*: EMF_061317_FINAL(PDF)

2.1.17 Provide guidance and direction to covered Bureau personnel on privacy and civil liberties matters applicable to the sharing of information in the ISE.

2.1.18 Ensure development and completion of training by covered Bureau personnel on the requirements of this circular and any additional guidance provided to ensure its proper implementation.

3.0 SUPERSESSION

None

4.0 AUTHORITIES AND REFERENCES

4.1 The Privacy Act of 1974, as amended (5 U.S.C. 552a)

4.2 Section 208 of the E-Government Act of 2002 (Public Law (Pub.L.) 107-347), September 30, 2003

4.3 Federal Information Security Modernization Act of 2014 (FISMA) (Public Law (Pub.L.) 113-283, S. 2521)

4.4 Title 31, Code of Federal Regulations (CFR), Subtitle A, Part 1, Subpart C, “Privacy Act”

4.5 Federal Register, Vol. 40, No. 132, at 40 FR 28948, July 9, 1975, OMB Privacy Act Implementation Guidelines and Responsibilities

4.6 Office of Management and Budget (OMB) Circular A-130, Managing Information as a Strategic Resource, July 27, 2016

4.7 OMB Memorandum M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, September 30, 2003

4.8 OMB Memorandum M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information, January 3, 2017

4.9 National Institute of Standards and Technology (NIST) Special Publication 800-122, Guide to Protecting the Confidentiality of PII, April 2010

4.10 NIST Special Publication 800-53, Revision 4, Appendix J, Privacy Controls, April 2013

4.11 NIST Special Publication 800-61, Computer Security Incident Handling Guide, August 2012

4.12 Treasury Directive 80-01, Department of the Treasury Information Technology (IT) Security Program, March 10, 2008

4.13 Treasury Directive 25-10, Information Sharing Environment Privacy and Civil Liberties Policy, June 21, 2013

4.14 Treasury Directive 25-09, Privacy and Civil Liberties Activities Pursuant to Section 803 of the Implementing Recommendations of the 9/11 Commission Act of 2007, P.L. 110-53, December 14, 2015

4.15 Treasury Directive 25-08, Safeguarding Against and Responding to the Breach of PII, December 22, 2009

4.16 Treasury Directive Publication 25-07, Privacy Impact Assessment (PIA) Manual, June 30, 2009

4.17 Treasury Directive 25-07, Privacy Impact Assessment (PTA)

4.18 Treasury Directive 25-04, The Privacy Act of 1974, as amended, January 27, 2014

4.19 Treasury Directive Publication (TD P) 25-04, "Privacy Act Handbook," June 2006

4.20 Treasury Acquisition Procedures Update No. 17-06, Acquisition Personnel Responsibilities in Support of Treasury's Privacy Program, April 11, 2017

4.21 Department of Justice, Overview of the Privacy Act of 1974

4.22 Circular No.50-00.8, Processing Requests Under the Freedom of Information and Privacy Acts, December 16, 2015

4.23 Circular No. 50-00.7, Record Systems Subject to the Privacy Act, January 21, 2011

4.24 Circular No. 40-00.14, Social Media Policy, December 20, 2016

4.25 Manual No. 10-08.35, IT Security Policy and Procedures Manual, September 13, 2010

4.26 BEP Standing Operating Procedure, Sending Secure Email from BEP, June 13, 2017

4.27 BEP Personnel Manual, Chapter 752, Appendix A. Table of Offenses and Penalties, September 1, 2016

5.0 DEFINITIONS

5.1 Activities: Combined actions that a BEP Office, Division, Section or individual takes in order to achieve a BEP mission or goal.

5.2 Agency: Means any executive agency or department, military department, Federal Government corporation, Federal Government-controlled corporation, or other establishment in the Executive Branch of the Federal Government (including the Executive Office of the President), or any independent regulatory agency.

5.3 Application: A software program hosted by an information system.

5.4 Authorization to Operate (ATO): BEP's Associate Director (AD) (Chief Information Officer) (CIO) decision to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security and privacy controls. Authorization also applies to common controls inherited by BEP information systems.

5.5 Breach: Suspected or actual loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for other than authorized purposes have access or potential access to PII whether in physical or electronic form.

5.6 Contractor: A private entity that enters into a contract with an agency.

5.7 Data: Information in a specific representation, usually as a sequence of symbols that have meaning.

5.8 Fair Information Practice Principles (FIPPs):[2] Set of eight principles that originate from the Privacy Act of 1974 and OMB Privacy Act Implementation Guidelines of 1975 (40 FR 28948) that form BEP's Privacy Controls. Privacy professionals use these principles as the framework for establishing privacy policies including (1) assuring that the use of technologies sustains and does not erode, privacy protections relating to the use, collection, and disclosure of personal information; and (2) assuring that personal information contained in the agency's systems of records is handled in full compliance with fair information practices as set forth in the Privacy Act.

5.9 Incident: Occurrence that actually or imminently jeopardizes, without lawful authority, the confidentiality, integrity, or availability of information or an information system; or constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.

5.10 Individual: A citizen of the United States or an alien lawfully admitted for permanent residence.

5.11 Information: Any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, electronic, or audiovisual forms.

5.12 Information Security: The protection of information and systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

5.13 Information System: A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

5.14 Information Security Risk: The risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation due to the potential for unauthorized access, use, disclosure, disruption, modification, or destruction of information and/or systems.

5.15 Information Technology: Equipment or interconnected system or subsystem of equipment, used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information.

5.16 Major Incident: A major incident is EITHER any incident that is likely to result in demonstrable harm to the national security interests, foreign relations, or the economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people. Agencies should determine the level of impact of the incident by using the existing incident management process established in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-61, Computer Security Incident Handling Guide. A major incident also occurs when a breach involves PII that, if exfiltrated, modified, deleted, or otherwise compromised, is likely to result in demonstrable

[2] The Fair Information Practice Principles are contained in OMB Circular A 130, Managing Federal Information as a Strategic Resource, Appendix II-2, July 28, 2016, *Available at*: A130.

harm to the national security interests, foreign relations, or the economy of the United States, or to the public confidence, civil liberties, or public health and safety of the American people.

5.17 Operations: A process or series of activities performed by multiple BEP personnel and/or technologies to produce a specific item or business function.

5.18 Personally Identifiable Information (PII): Information that can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc., alone, or when combined with other personal or identifying information that is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.

DEFINITIONS (CONTINUED)

5.19 Privacy and Civil Liberties Impact Assessment (PCLIA): An analysis of how information is handled to (1) ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy, (2) to determine the risks and effects of creating, collecting, using, processing, storing, maintaining, disseminating, disclosing, and disposing of information in identifiable form in an electronic information system, and (3) to examine and evaluate protections and alternate processes for handling information to mitigate potential privacy concerns. A PCLIA is both an analysis and a formal document detailing the process and the outcome of the analysis. (Attachment A)

5.20 Privacy Controls: Administrative, technical, and physical safeguards employed within organizations to protect and ensure the proper handling of PII.[3]

5.21 Privacy Posture: The status of the information systems and information resources (e.g., personnel, equipment, funds, and information technology) within an organization based on information assurance resources (e.g., people, hardware, software, policies, procedures) and the capabilities in place to comply with applicable privacy requirements and manage privacy risks and to react as the situation changes.

5.22 Privacy Threshold Analysis (PTA): Tool used to determine whether a PCLIA is required under Section 208 of the E-Government Act of 2002. The PTA is used to help the program managers/offices evaluate the information/data in the system and make a risk-based determination about how to manage and secure the information/data (e.g., the Privacy Posture), as required by the Privacy Act and other federal statutes, regulations and Departmental policies. The PTA is also used to identify the need for additional privacy documentation (e.g., System of Records Notice), and to determine the overall privacy posture of the system, project, or program. PTA templates are provided to program managers and system owners at the beginning stages of the System Development Life Cycle (SDLC) process.

5.23 Risk: A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically is a function of: (1) the adverse impact, or magnitude

[3] NIST Special Publication (SP) 800-53, Rev. 4, Appendix J, *Available at:* APPENDIX J.

of harm, that would arise if the circumstance or event occurs; and (2) the likelihood of occurrence.

5.24 Risk Assessment: The process of identifying risks to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of a system.

5.25 Risk Management: The program and supporting processes to manage risk to agency operations (including mission, functions, image, reputation), agency assets, individuals, other organizations, and the Nation, and includes: establishing the context for risk-related activities; assessing risk; responding to risk once determined; and monitoring risk over time.

5.26 Routine Use: The use of a Privacy Act record compatible with the purpose for which it was created and in accordance with the privacy system announcement in the Federal Register.

5.27 Sensitive PII: PII, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Complete social security numbers (SSN), alien registration numbers (A-number) and biometric identifiers (such as fingerprint, voiceprint, or iris scan) are considered Sensitive PII even if they are not coupled with additional PII. Additional examples include any grouping of information that contains the individual's name or other unique identifier **plus** one or more of the following elements:

- Driver's license number, passport number, or truncated SSN (such as last-4 digits);
- Date of birth (month, day, **and** year);
- Citizenship or immigration status;
- Financial information such as account numbers or Electronic Funds Transfer information;
- Medical information; and
- System authentication information such as mother's maiden name, account passwords or personal identification numbers (PINs).

NOTE: Other PII may be "sensitive" depending upon its context, such as a list of employees with less than satisfactory performance ratings or an unlisted home address or phone number. In contrast, a business card or a public phone directory of agency employees contains PII but is not necessarily sensitive.

5.28 Social Media: Any online tool or application or web-based technology that goes beyond simply providing information, instead allowing collaboration, dialogue, interaction, and create, organize, edit, comment on, combine, and share content. Examples of social media include: blogs; microblogs; wikis; photo and video sharing; podcasts; virtual worlds; social networking; social news and bookmarking; web conferencing and webcasting.

5.29 System Development Life Cycle (SDLC): The SDLC is the multistep process that starts with the initiation, analysis, design, and implementation of an information technology system, and continues through the maintenance and disposal of the system.

5.30 System of Records: Group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifier assigned to the individual.

5.31 System of Records Notice (SORN): Formal notice to the public published in the Federal Register that identifies the purpose for which PII is collected, from whom and what type of PII is collected, how the PII is shared externally (routine uses), and how to access and correct any PII maintained by the Bureau.

5.32 System Owner: BEP Office Chief responsible for the use of the program, IT system and who implements the legal information resources management requirements of the Department, such as per the guidance contained in OMB Memorandum 03-22, dated September 26, 2003.

6.0 RESPONSIBILITIES

6.1 The Assistant Secretary for Management (ASM) of the Department of the Treasury (Treasury) is the Senior Agency Official for Privacy (SAOP) and the Chief Privacy and Civil Liberties Officer (PCLO) of BEP.

6.2 The Deputy Assistant Secretary for Privacy, Transparency, and Records (DASPTR) of Treasury is the SAOP/PCLO's principal advisor on issues related to privacy and civil liberties. The DASPTR leads Treasury's Office of Privacy and Transparency and Records (PTR), and provides the SAOP/PCLO with day-to-day support in executing SAOP/PCLO duties.

6.2.1 Treasury's PTR, Privacy and Civil Liberties:

6.2.1.1 Reports to the DASPTR.

6.2.1.2 Manages PTR's Privacy and Civil Liberties.

6.2.1.3 Supports BEP's Government Information Specialist for Privacy.

6.2.1.4 Provides privacy and civil liberties training to BEP.

6.2.1.5 Ensures that BEP complies with all privacy and civil liberties-related federal laws and regulations and government and Treasury wide policies.

6.2.1.6 Reviews BEP's Annual Privacy, Data Mining, and Section 803 Reports before consolidation with Department Offices and other Bureaus and forwarding it to OMB, DHS, and Congress as appropriate.[4]

[4] The Consolidated Privacy Reports provide Congress and the public with a comprehensive overview of Treasury's privacy compliance and oversight activities for the following reports: (1) The Annual Privacy Report required by Section 522(a) of the Consolidated Appropriations Act of 2005; (2) The Data Mining Reporting Act requirement contained in Section 803 of the Implementing Recommendations of the 9/11 Commission Act of 2007, 42 U.S.C. § 2000ee–3; and, (3) The Semi-Annual Privacy and Civil Liberties report required under Section 803 of the Implementing Recommendations of the 9/11 Commission Act of 2007. These reports provide awareness into the Department's complaints of privacy violations, training, and overall privacy compliance posture.

6.2.1.7 Provides oversight and assists BEP to ensure compliance with the guidelines for conducting PCLIAs.

6.2.1.8 Consults with and assists appropriate BEP entities to develop policies, procedures, and standards necessary to comply with ISE Privacy Guidelines (per Treasury Directive Publication TD P 25-10).[5]

6.3 Director, BEP:

6.3.1 Has responsibility for the overall implementation of the privacy and civil liberties program at BEP.

6.3.2 Delegates the privacy and civil liberties responsibilities to the Associate Director (Chief Information Officer).

6.4 Associate Director (Chief Information Officer) (CIO):

6.4.1 Acts on behalf of the Director to ensure that BEP's privacy and civil liberties program appropriately complies with federal law and regulations and government and Treasury-wide policies.

6.4.2 Re-delegates BEP's privacy and civil liberties program to the Office of Critical Infrastructure and IT Security.

6.4.3 Issues all Security Authorizations (SA), for the operation of BEP's information systems.

6.4.4 Has responsibility for BEP's operations and assets based on the implementation of an agreed-upon set of security and privacy controls.

6.4.5 Has responsibility for the security of the operation of an assessed information system and officially declares that the information system is ATO.

6.5 The Chief of the Office of Critical Infrastructure & IT Security (OCIITS):

6.5.1 Reports to the AD (CIO) on privacy and civil liberties matters.

6.5.2 Supervises BEP's Manager, OCIITS Cybersecurity Policy and Compliance Division (CPCD).

6.5.3 Identifies and oversees implementation of privacy and civil liberties requirements in BEP in accordance with Federal laws, regulations, and policies.

6.5.4 Maintains a system inventory of all major information systems that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII in accordance with the Federal Information Security Modernization Act of 2014 (FISMA) (Public Law (Pub.L.) 113-283, S. 2521). This inventory allows BEP to regularly review its PII and ensure, to the extent reasonably practicable, that such PII is accurate, relevant, timely, and complete; and to allow the agency to reduce its PII to the minimum necessary for the proper performance of authorized agency functions.

[5] Treasury Directive Publication TD P 25-10, Information Sharing Environment (ISE) and Civil Liberties Policy: Implementation Plan, May 2013. *Available at*: TD-P-25-10-Information-Sharing-Enviornment-and-Civil-Liberties-Policy-Implementation-Plan (PDF)

6.5.5 Manages the PTA and PCLIA compliance programs for new or updated IT systems and/or information programs or projects that collect, maintain, or disseminate information that is in an identifiable form from or about members of the public. Serves as the Reviewing Official for all PCLIAs. Delegates this activity to the CPCD Manager.

6.5.6 Manages all BEP information and information systems security measures that protect BEP assets, resources, and personnel from unauthorized access, use, disclosure, disruption, modification, or destruction to protect personal privacy.

6.5.7 Manages the accuracy and submission of all annual or semi-annual Privacy Reports to PTR for transmittal to OMB, DHS, or Congress as appropriate in accordance with Section 208 of the E-Government Act of 2002 and other federal laws, policies, and mandates. Delegates this activity to the CPCD Manager.

6.5.8 Manages information security, privacy, records management, public transparency, and supply chain security issues for all resource planning and management activities throughout the system development life cycle so that risks are appropriately managed.

6.5.9 Ensures that a capability is maintained for privacy incident response and reporting in accordance with policy to the Bureau CSIRC and, when warranted, to the Treasury CSIRC (TCSIRC). Delegates this activity to the CPCD Manager.

6.5.10 Applies appropriate safeguards to protect the confidentiality of PII based on the PII confidentiality impact level. Delegates this activity to the CPCD Manager.

6.5.11 Reviews PII holdings to ensure that these holdings are accurate, relevant, timely and complete, and reduce their holdings of PII to the minimum necessary to effectively administer Bureau programs. Delegates this activity to the CPCD Manager.

RESPONSIBILITIES (CONTINUED)

6.6 The OCIITS's Cybersecurity Operations Division (COD) and the Cybersecurity Policy and Compliance Division (CPCD):

6.6.1 Serves as the initial point of contact in the privacy compliance process for new or updated IT systems, technologies, programs, activities, social media initiatives, information collections, or operations. COD also ensures, on behalf of system owners, that information system security plans are developed. CPCD ensures that IT systems are tested, validated, implemented, and maintained in accordance with Federal law, regulations, and guidance, and Department of the Treasury and BEP information security policy procedures. CPCD also supports the IT and Privacy/PII incident management process. CPCD privacy support includes:

6.6.1.1 Managing the Government Information Specialist for Privacy.

6.6.1.2 Collaborating with the Program Manager/System owner to prepare and submit a PTA to the Government Information Specialist for Privacy to assess any system, program, or initiative to (1) determine the privacy posture and

required documentation, and (2) ensure the minimization or anonymization of PII prior to testing, training, research, and/or operational deployment;

6.6.1.3 Providing IT security program oversight to ensure compliance with IT security policy and procedures;

6.6.1.4 Staffing and maintaining an Incident Response team known as the CSIRC to respond to, investigate, and collaborate with the Government Information Specialist for Privacy to mitigate detected and reported actual and suspected privacy and IT security incidents. Delegates reporting responsibilities for privacy/PII incidents to the Government Information Specialist for Privacy;

6.6.1.5 In collaboration with the Government Information Specialist for Privacy, implementing and maintaining the National Institute of Standards and Technology (NIST) Risk Management Framework (RMF) in accordance with NIST special publications that govern privacy and security controls within BEP IT systems. Additionally, CPCD uses these practices and procedures to assess information security risks;

6.6.1.6 Applying appropriate safeguards to protect the confidentiality of PII based on the PII confidentiality impact level;

6.6.1.7 Testing and evaluating the effectiveness of policies, procedures, and security and privacy controls; and

6.6.1.8 Managing the Bureau inventory of PII holdings.

6.7 The BEP Government Information Specialist for Privacy (GISP):

6.7.1 Reports to the Chief of OCIITS and Division Manager of Cybersecurity Policy and Compliance Division.

6.7.2 Ensures that BEP's programs, activities, social media, information systems, information technologies, or operations sustain, and do not erode, privacy and civil liberties protections relating to the use, collection, and disclosure of PII.

6.7.3 Evaluates the impact of legislative and regulatory proposals involving collection, use, and disclosure of PII by the federal government on BEP activities.

6.7.4 Ensures that Bureau privacy policies on websites used by the public contain appropriate language to explain Bureau information handling practices in accordance with Section 208 of the E-Government Act of 2002.

6.7.5 In collaboration with the Program Office and appropriate BEP stakeholders at the SDLC stage, conducts and completes privacy compliance documentation (e.g., SORNs, PLCIAs, PTAs) for new or updated BEP programs, activities, social media, information systems, information technologies, or operations in accordance with federal law and regulation. Serves as the Privacy Official for PCLIAs and coordinates stakeholder approval and obtain signatures from the Reviewing Official and System Owner/Program Manager.

6.7.6 Ensures that BEP programs, activities, social media, information systems, information technologies, or operations only create, collect, use, process, store,

maintain, disseminate or disclose PII that is directly relevant and necessary to accomplish a legally authorized purpose, and should maintain PII for as long as is necessary to accomplish the purpose.

6.7.7 Ensures that programs activities, social media, information systems, information technologies, or operations, policies and procedures involving and privacy and civil liberties considerations are addressed in an integrated and comprehensive manner.

6.7.8 Develops de-identification techniques to remove, reduce, or anonymize PII during IT System testing phases, training, and/or during research and development (R&D) activities. These measures include but are not limited to removing/obscuring enough PII in such a manner (e.g., by redaction, one-way cryptographic function (hashing), etc.) that the remaining information does not identity an individual.

6.7.9 Ensures that new or updated information systems contain measures to migrate, segregate, or delete PII/records in accordance with the prescribed NARA-approved records retention schedule.

6.7.10 Serves as BEP's primary point of contact for privacy and civil liberties general matters and PII-related incidents. Prepares incidents reports and submits them to TCSIRC via the Treasury Incident Reporting System within one business day after discovery. (Attachment B)

6.7.11 Manages and handles privacy and civil liberties incidents affecting BEP activities, social media, information systems, information technologies, or operations including but not limited to:

6.7.11.1 Ensuring that all BEP employees and contractors report all suspected or confirmed PII-related incidents within one hour of discovery to the IT Service Desk and their supervisor;

6.7.11.2 Performing an administrative investigation, notification, mitigation for all privacy and civil liberties incidents;

6.7.11.3 Compiling privacy and civil liberties reports to Treasury's PTR Privacy and Civil Liberties for all suspected and/or confirmed PII incidents;

6.7.11.4 Informing the Treasury's PTR Privacy and Civil Liberties of the status of a potential or confirmed privacy incident when needed (e.g., sensitive issues, multiple Bureau incidents);

6.7.11.5 Notifying the BEP Office of Acquisition of any privacy incident that involves government-issued credit cards and other Chief Financial Officer (CFO) Directorate Designated Financial Systems Assess the likely risk of harm posed by the privacy incident (e.g., low, moderate, or high impact) to facilitate mitigation;

6.7.11.6 Notifying the employee's supervisor and appropriate Human Resource Officer or their designee, of all incidents reported to the TCSIRC that

involve the compromise or loss of a system or PII to address whether the circumstances of the incident suggest that corrective action is necessary;

6.7.11.7 Serving as a member of the BEP Incident Response Team in order to address and mitigate major PII data incidents and to assist in coordinated responses with key BEP stakeholders (e.g., OCIITS, Office of Chief Counsel [OCC], CFO, and Office of External Relations [OEX]) when appropriate. These stakeholders address matters such as notice, credit monitoring, and external outreach to OMB, Congress, Media, and Privacy Advocacy Groups, when appropriate; and

6.7.11.8 Composing and/or assisting associated office(s) in preparing documents (e.g., incident/breach notification letters) as needed.

6.7.12 Developing, maintaining, and providing role-based and/or targeted privacy awareness training for BEP employees and contractors when the need arises or upon request.

6.7.13 Apprising employees and contractors about available privacy and security resources, such as products, techniques, or expertise (e.g., Secure Email Transmission Tools).

6.7.14 Responding to all privacy-related complaints submitted to the Privacy@BEP.Gov email address or other communication mechanisms within 48 hours. Collaborate with the Privacy Act Officer on any requests for redress from individuals seeking to correct and/or amend information contained in a Privacy Act System of Records.

6.7.15 Initiating the BEP response and provide performance metrics and information to all privacy-related reports and/or data calls (e.g., FISMA, Data Mining) from external stakeholders (e.g., OMB, Congress, and Treasury).

6.7.16 Conducting the inventory of PII holdings and transmits the information to PTR annually or upon request.

6.8 The Office of Chief Counsel is BEP's Privacy Act Officer and oversees the implementation of BEP's Privacy Act Program. For more information please see Circular No. 50-00.7, Record Systems Subject to the Privacy Act, January 21, 2011.

6.9 System Owners/Office Chiefs:

6.9.1 Manage the overall procurement, development, integration, modification, operation, maintenance, and retirement of an information system.

6.9.2 Assist the Government Information Specialist for Privacy by providing information to assist in developing any required privacy compliance documentation (e.g., PTA, PCLIA, SORN) pertaining to any new or revised system, program or Bureau initiative.

6.9.3 Determine the use and access restrictions for information systems.

6.9.4 Maintain an accounting of the date, nature, and purpose of each disclosure of records containing PII (except for disclosures within the Department of the Treasury

to individuals with a need-to-know the information). This accounting includes the name and address of the person or agency to whom the disclosure is made.

6.9.5 Retain records in accordance with an approved records disposition/retention schedule and dispose of such records in a manner that will not compromise PII.

6.9.6 Address any corrective action(s) as directed by the Government Information Specialist for Privacy or following consultation with the Office of Human Resources (OHR) and OCC pertaining to employees or contractors under their jurisdiction that cause a Privacy/PII incident as described in Section 2 above. The individual may be subject to BEP Personnel Manual, Chapter 752, Appendix A. Table of Offenses and Penalties (Page 315), September 1, 2016.[6]

6.10 System Managers:

6.10.1 Establish, maintain, revise, or delete systems of records in accordance with applicable laws and regulations relating to privacy and Federal records.

6.10.2 Establish administrative and physical controls to ensure the protection of records systems from unauthorized access or disclosure, and from physical damage or destruction.

6.10.3 Assist the Government Information Specialist for Privacy by providing technical information/data to assist in developing any required privacy compliance documentation (e.g., PTA, PCLIA, SORN) pertaining to any new or revised system, program, or Bureau initiative.

6.10.4 Ensure that all employees and contractors that maintain access to BEP IT systems or resources take mandatory annual Treasury PTR Privacy and Civil Liberties Awareness Training offered via the BEP Integrated Talent Management System (ITMS).

6.10.5 Review all record holdings and activities that involve SSNs (SSNs) to determine whether a business or statutory need remains to continue using the full or truncated SSN or migrate to a less sensitive personal identifier.

6.10.6 Verify the accuracy, relevance, timeliness, and completeness of the PII provided at the point of collection, to the extent practical.

6.10.7 Submit a PTA to the Government Information Specialist for Privacy to assess BEP activities, social media, information systems, information technologies, or operations to (1) determine the privacy posture and required documentation, and (2) ensure the minimization or anonymization of PII prior to testing, training, research, and operational deployment.

6.11 BEP Contracting Officers (CO) in the Office of Acquisition (OA)

[6] BEP Personnel Manual, *Available at*: http://insite/Documents/Directives/Manual%20M-60-1.pdf#search=personnel%20manual%27.

6.11.1 Ensure via the Contracting Officer's Representative (COR) that all contractors and subcontractors complete Treasury PTR Privacy and Civil Liberties awareness training prior to the individual accessing data, including PII, on the BEP Network, in IT systems, or within other information collections. The CO shall report all non-completions for subsequent annual training to the GISP upon request.

6.11.2 Ensure that all procurements that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII contain contract language/clauses as prescribed by Federal Acquisitions Regulations (FAR 24.302(b). (Attachment C)

6.12 BEP Employees and Contractors are responsible for:

6.12.1 Completing initial and annual privacy awareness training when assigned via a Treasury/BEP learning management tool.

6.12.2 Complying with federal laws and regulations and government and Treasury wide policies concerning privacy and civil liberties.

6.12.3 Reporting all suspected or confirmed Privacy/PII incidents to their supervisor and then to the IT Service Desk within 1-hour of discovery.

6.12.4 Responding promptly to CPCD Personnel that seek additional information pertaining to any suspected or confirmed incident.

6.12.5 Encrypting all emails containing PII transmitted outside of the Treasury/BEP Network (e.g., .com, .net, .edu, .org email domains and/or other federal, state, local, or tribal agencies email addresses).

6.12.6 Following additional best practices and procedures to safeguard PII entrusted to them in the performance of their official duties (Attachment D).

7.0 OFFICE OF PRIMARY RESPONSIBILITY

Office of Critical Infrastructure and IT Security

<electronically approved>
Leonard R. Olijar
Director

ATTACHMENT A

Department of the Treasury/BEP Privacy and Civil Liberties Impact Assessments (PCLIAs)

Section 208 of the E Government Act of 2002 created the requirement to conduct Privacy Impact Assessments (PIA) for systems that process personal identifiable information (PII) on members of the public. Treasury designed a PIA template as a decision tool that also addresses Civil Liberties concerns The PCLIA identifies and mitigates privacy risks, while notifying the public about:

- What PII Treasury/BEP is collecting;
- Why the PII is being collected; and
- How the PII will be collected, used, accessed, shared, safeguarded and stored.

It is required for new systems, those systems undergoing modification or enhancement, and the Paperwork Reduction Act electronic collections of information. OMB Memorandum 03-22, dated September 26, 2003, contains guidance for conducting PCLIAs as well as procedures for processing and posting completed assessments.

A PCLIA should accomplish three goals:

- Ensure conformance with applicable legal, regulatory, and policy requirements for privacy;
- Determine the risks and effects; and
- Evaluate protections and alternative processes to mitigate potential privacy risks.

Treasury/BEP conducts a PCLIA when:

- Developing or procuring any new technologies or systems that handle or collect PII on members of the public;
- Creating a new program, system, technology, or information collection that may have privacy implications;
- Updating a system that results in new privacy risks; and
- Issuing a new or updated rulemaking that entails the collection of PII on members of the public.

The PCLIA contains the following sections:

- An overview of its purpose and functions;
- A description of the information collected;
- A description of the how information is maintained, used, and shared;
- An assessment of whether the system or project is in compliance with federal requirements that support information privacy; and

- An overview of the redress/complaint procedures available to individuals who may be affected by the use or sharing of information by the system or project.

BEP Program Managers and System Owners will provide pertinent information to the Government Information Specialist for Privacy, who will produce any required PCLIAs and submit them to the Office of Chief Counsel (OCC) for a legal review. All PCLIAs will be signed by the System Owner, Government Information Specialist for Privacy, and the Reviewing Official from OCIITS. OCC will review the completed document for any legal implications resulting from posting the document publicly. Final versions designated for public posting will be available at: BEPfoialibrary. Program Managers and System Owners should view these PCLIAs as a resource and to learn the breadth of content for collaboration purposes.

Department of the Treasury/BEP Privacy Threshold Analysis

The purpose of the Privacy Threshold Analysis (PTA) is to help BEP evaluate the information/data in the system and make the appropriate determination about how to manage and secure the information/data in accordance with federal laws, statutes, regulations, and Departmental policies.

Thus, the self-explanatory PTA Template helps BEP determine if the data in the information system includes information about individuals, e.g., personally identifiable information (PII), which will require BEP to conduct a PCLIA.

The PTA contains sections to obtain the following information:

Section 1: General Privacy Posture Assessment to determine:

1. Type of project/program/system.
2. Reason for the submission.
3. General description of the project/update and its purpose.
4. Status of the project/program.
5. Whether the project/program collects PII and on what population.
6. Whether the project/program collect SSNs.
7. A general description of the way the project/program relates to individuals.
8. The type of PII the project/program collects, maintains, or shares.
9. Security Authorization/Certification and Accreditation Status.
10. Previous PIAs and publication date.
11. Privacy Act System of Records Notice (SORN) requirement and/or status.
12. Associated forms (if any).
13. Estimated number of records containing PII in the system.

Section 2: Risk Management/PII Confidentiality Impact Level Categorization, which will be completed by the Government Information Specialists for Privacy. All PII is not created equal. PII should be evaluated to determine its PII confidentiality impact level in order to provide appropriate safeguards to the PII. The "Factors" below will be scored to provide a PII confidentiality impact level (e.g., Low, Moderate, or High) in order to indicate the potential harm that could result to individuals and/or the organization if PII were inappropriately accessed, used, or disclosed.

1. Factor 1 - Identifiability
2. Factor 2 - Quantity of PII
3. Factor 3 - Data Field Sensitivity
4. Factor 4 - Obligation To Protect Confidentiality
5. Factor 5 - Access to and Location of PII
6. Factor 6 - Context of Use

BEP Office of Critical Infrastructure and IT Security, Cyber Security Policy and Compliance Division (OCIITS/CPCD) contractors will collaborate with Program Managers and System Owners to complete the initial PTA and provide the partially-completed document to the Government Information Specialists for Privacy for the PII Risk Categorization and final completion.

ATTACHMENT B

BEP PRIVACY/PII INCIDENT RESPONSE PROCESS AND PROCEDURES

The Bureau of Engraving and Printing (BEP/Bureau) relies heavily on the confidentiality, integrity, and availability of IT resources to support day-to-day operations. Trends toward increasing system interconnections raise both productivity and risk of threats such as computer viruses and intrusions. These threats also raise privacy risks as the Bureau increases its use of sensitive datasets containing Personally Identifiable Information (PII) on employees, contractors, and members of the public. Utilizing the foundation established through the Treasury Information Security Program as documented in Department of the Treasury Information Technology (IT) Security Program Treasury Directive Publication (TD P) 85-01, BEP established supplemental incident response procedures to accomplish this task. Thus, as outlined in TD P 85-01, Appendix G, *The Departmental Incident Response Plan*, BEP developed a Computer Security Incident Response Capability (CSIRC) that aligns with guidance from OMB, the Department of Homeland Security, National Cybersecurity and Communications Integration Center (NCCIC) (*also known as* US-CERT), Treasury policies, and National Institute of Standards and Technology (NIST) incident response methodology.

The BEP CSIRC Response Team

Primary Team: BEP Cybersecurity Policy and Compliance Division (CPCD) employees and contractors, which includes the Government Information Specialist for Privacy, are responsible for assessing and determining whether an actual incident occurred. This team is also responsible for mitigating any risks associated with confirmed incidents.

Extended Team: Consists of the CPCD team, plus stakeholders from the following BEP Offices in response to a major incident:

1. Office of Chief Counsel (OCC) – For legal guidance.
2. Office of External Relations (OEX) – Responsible for managing all communications with the public regarding BEP (e.g., press releases, questions and answers, talking points, federal entity outreach, and inquiries); and
3. Office of Acquisition (OA) – Responsible for assisting the Chief Information Officer (CIO) Directorate staff in obtaining Credit Monitoring Services, if warranted.

Requirements

BEP employees and contractors must:

1. Report all suspected or confirmed PII-related incidents to their supervisor and to the IT Service Desk link on In$ite or by calling (202)874-3010 within one hour of discovery.

2. Encrypt all emails containing PII transmitted outside of the Treasury/BEP Network (e.g., .com, .net, .edu, .org email domains and/or other federal, state, local, or tribal agencies email addresses).

Available Resources

Employees and contractors shall use the BEP Secure Transmission (Axway) Tool in MS Outlook to encrypt email and attachments containing PII transmitted outside of the Treasury/BEP Network. Recipients of the email will have 72 hours to retrieve the encrypted email before it self-deletes from their mailbox.

In instances where 72 hours may not provide ample time for the recipient to retrieve the email (e.g., commercial entities, military installations), employees and contractors may contact the Government Information Specialist for Privacy in order to obtain additional secure transmission methods (e.g., MS Office, Adobe, and WinZip Encryption methods) or seek guidance regarding safeguarding PII.

The Incident Response Process

1. The Government Information Specialist for Privacy and/or IT Security Specialists (CPCD Incident Response Team) receives incident notifications from the IT Service Desk, employees, contractors, or Treasury CSIRC (for unencrypted email transmissions outside of the Treasury/BEP Network) and then:

    a. Investigates/analyzes the circumstances surrounding the suspected incident to confirm whether it involved PII and to confirm the loss of the information;

    b. Provides the employee/contractor and their supervisor guidance to mitigate the incident if possible (e.g., recall emails, confirm recipients, re-image computers containing malware, state the whereabouts of hardcopy PII document, etc.);

    c. Advises the employee/contractor and their supervisor whether the incident constitutes a PII breach and whether CPCD Incident Response Team will create an official incident report.

2. Once a breach is confirmed, the CPCD Incident Response Team creates an incident report in the Treasury CSIRC Reporting System that provides pertinent information such as:

    a. Incident descriptive title and number;

    b. Date and time of the incident and when reported to the CPCD Incident Response Team;

    c. Whether the incident is major or minor;

    d. Name of individual that caused the incident

    e. Number of individuals impacted by the incident;

    f. Summary of the incident and additional comments;

    g. Type and number of exposed PII records;

    h. Impacted systems (if applicable);

    i. Contact information for CPCD Incident Response Team; and

j. Whether the incident is open/closed.

3. Additional Notifications:

   a. Supervisors;

   b. Office of Human Resources (OHR) (for corrective action purposes);

   c. Office of Acquisition (OA) – for Contracting Officer Representative-related incidents); and

   d. Office of Chief Counsel (OCC).

ATTACHMENT B (CONTINUED)

4. Treasury CSIRC reviews all BEP incident reports and assists in or performs mitigation efforts on electronic breaches if necessary. Treasury CSIRC also reports all PII incidents to DHS/US-CERT within one hour of receipt as required. US-CERT may notify external Federal stakeholders (e.g., OMB, Congress) when warranted.
5. Prior to closing a Privacy/PII incident, the Government Information Specialist for Privacy will provide employees and contractors responsible for PII incidents corrective actions that include PII-safeguarding guidance, information, and/or refresher Privacy Awareness Training. Additional corrective actions are addressed by the employee's supervisor, OHR, and/or OCC when necessary.
6. The CPCD Incident Response Team will review the circumstances and associated risk to determine if notification or additional protective measures (e.g., credit monitoring services) will be provided to the impacted individuals. The BEP Senior Executive Team (SET) will be consulted to address these measures during major incidents.
7. Once the CPCD Incident Response Team determines that mitigation efforts, notification (if required), and any additional activities are completed, the employee/contractor and their supervisor receives an Incident Closure Summary email explaining:

   a. The circumstances of the incident;

   b. Policies that the individual violated and are required to follow;

   c. PII safeguarding reminders; and

   d. Notice of incident closure.

8. The CPCD Incident Response Team closes the incident in the Treasury CSIRC Incident Reporting System.

ATTACHMENT C

FAR Subpart 1024.3 Contract Clauses

Subpart 24.3—Privacy Training

24.301 Privacy training.

(a) Contractors are responsible for ensuring that initial privacy training, and annual privacy training thereafter, is completed by contractor employees who–

(1) Have access to a system of records;

(2) Create, collect, use, process, store, maintain, disseminate, disclose, dispose, or otherwise handle personally identifiable information on behalf of the agency; or

(3) Design, develop, maintain, or operate a system of records (see FAR subpart 24.1 and 39.105).

(b) Privacy training shall address the key elements necessary for ensuring the safeguarding of personally identifiable information or a system of records. The training shall be role-based, provide foundational as well as more advanced levels of training, and have measures in place to test the knowledge level of users. At a minimum, the privacy training shall cover–

(1) The provisions of the Privacy Act of 1974 (5 U.S.C. 552a), including penalties for violations of the Act;

(2) The appropriate handling and safeguarding of personally identifiable information;

(3) The authorized and official use of a system of records or any other personally identifiable information;

(4) The restriction on the use of unauthorized equipment to create, collect, use, process, store, maintain, disseminate, disclose, dispose, or otherwise access personally identifiable information;

(5) The prohibition against the unauthorized use of a system of records or unauthorized disclosure, access, handling, or use of personally identifiable information; and

(6) Procedures to be followed in the event of a suspected or confirmed breach of a system of records or unauthorized disclosure, access, handling, or use of personally identifiable information (see Office of Management and Budget guidance for Preparing for and Responding to a Breach of Personally Identifiable Information).

(c) The contractor may provide its own training or use the training of another agency unless the contracting agency specifies that only its agency-provided training is acceptable (see 24.302(b)).

(d) The contractor is required to maintain and, upon request, to provide documentation of completion of privacy training for all applicable employees.

(e) No contractor employee shall be permitted to have or retain access to a system of records, create, collect, use, process, store, maintain, disseminate, disclose, or dispose, or otherwise handle personally identifiable information, or design, develop, maintain, or operate a system of records, unless the employee has completed privacy training that, at a minimum, addresses the elements in paragraph (b) of this section.

24.302 Contract Clause.

(a) The contracting officer shall insert the clause at FAR 52.224-3, Privacy Training, in solicitations and contracts when, on behalf of the agency, contractor employees will–

(1) Have access to a system of records;

(2) Create, collect, use, process, store, maintain, disseminate, disclose, dispose, or otherwise handle personally identifiable information; or
(3) Design, develop, maintain, or operate a system of records.
(b) When an agency specifies that only its agency-provided training is acceptable, use the clause with its Alternate I.

Additional Language for Requirements Documents such as the Statement of Work (SOW) or Performance Work Statement (PWS)

(a) The following are minimum privacy requirements that shall be addressed within the requirements document, unless otherwise addressed within a Bureau contracting activity clause:

(1) Require the contractor to cooperate with and exchange information with Treasury officials, as determine necessary by Treasury, in order to effectively report and manage a suspected or confirmed breach[7];

(2) Require contractors and subcontractors (at any tier) to properly encrypt PII in accordance with OMB Circular No. A-130 and other applicable policies and to comply with Treasury specific policies for protecting PII;

(3) Require regular training for contractors and subcontractors (at any tier) on how to identify and report a breach (see FAR subpart 243 and 1024.3 for Privacy Training requirements);

(4) Require contractors and subcontractors (at any tier) to repo11 a suspected or confirmed breach in any medium or form, including paper, oral, and electronic, as soon as possible and without unreasonable delay; consistent with Treasury's incident management policy, Bureau supplemental plan, and US-CERT notification guidelines;

(5) Require contractors and subcontractors (at any tier) to maintain capabilities to determine what Federal information was or could have been accessed and by whom, construct a timeline of user activity, determine methods and techniques used to access Federal information, and identify the initial attack vector;

(6) Allow for an inspection, investigation, forensic analysis, and any other action necessary to ensure compliance with this 0MB memorandum M-17-12, Treasury's breach response plan, Bureau supplemental plan, if applicable, and to assist with responding to a breach;

(7) Identify roles and responsibilities, in accordance with 0MB memorandum M-17-12 and the Treasury's breach response plan;

(8) Explain that a report of a breach shall not, by itself: be interpreted as evidence that the contractor or its subcontractor {at any tier) failed to provide adequate safeguards for PII; and

[7] Suspected or actual loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for other than authorized purposes have access or potential access to PII whether in physical or electronic form.

(9) Require as part of the expiration or termination of the contract compliance with Treasury's requirements regarding the return and/or disposal of PII obtained under the contract.

ATTACHMENT D

Additional Best Practices and Procedures for Safeguarding Personally Identifiable Information (PII)

- Quality Control – There are times when employees and contractors must distribute large amounts of PII in tables, spreadsheets, or via mass mailings. When practical, seek a secondary review from co-workers to catch errors before transmitting emails and conducting mass mailings.
- Ensure that you use the MS Outlook Secure Transmission Tool as described in Attachment B and in BEP's Standard Operating Procedure (SOP) for Sending Secure Email.
- Physically secure PII in your possession (locked cabinets, desk drawers, safes, etc.).
- Remove PIV cards from readers prior to departing your workstation.
- Don't email work-related PII to Gmail, Hotmail, or other personal accounts for convenience.
- Restrict access in shared drives (e.g., SharePoint) to those with a need-to-know.
- Safeguard sensitive content or embarrassing facts about individuals that may arise during business operations.
- Do not discuss or share personal information about other individuals in open settings or with those that do not have a need-to-know the information in the performance of official duties.
- Remember to pick up sensitive printed documents in a timely manner from copiers/scanners/fax machines.
- Do not seek Social Security Numbers (SSNs) unless there is a legitimate need to use the data as a personal identifier when no other would serve the business purpose.
- Do not install non-BEP issued mobile devices (including flash/thumb drives) to BEP assets.
- Do not discard PII in trash or recycling receptacles. Use cross-cut shredders or the "burn bag" process.
- Beware of emails that appear to originate from legitimate sources but are actually "Phishing Attacks." Use care when reviewing emails that do not originate from a ".gov" email domain. Use MS Outlook/View/Reading Pane to view (single click) an email's header/content without opening the email.
- Report all attempts to gain unauthorized access to data, especially confidential data or PII such as SSNs.