Department of the Treasury

Bureau of Engraving and Printing

Privacy and Civil Liberties Impact Assessment for the Use of Third-Party Social Media Websites for Public Engagement

Box Content Management/Enterprise Cloud Content Collaboration Platform

November 14, 2017

Section 1: Introduction

The Department of the Treasury ("Treasury"), Bureau of Engraving and Printing ("BEP"/Bureau) uses third-party social media websites and applications to engage in dialog with members of the public to promote transparency, improve public access to government information, and encourage public participation and collaboration. In accordance with the President's Memorandum on Transparency and Open Government[1], the Director of the Office of Management and Budget's (OMB) Open Government Directive Memorandum,[2] OMB Circular No. A-108, Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act,[3] and BEP's Social Media Policy,[4] BEP upholds the principles of transparency, participation, and collaboration to foster a culture of open government throughout the Bureau's use of third party-party social media websites and applications. The Bureau uses the following types of third-party social media:

1) Third-party websites and applications that facilitate one-way and two-way interaction[5] between BEP and the public. Members of the public typically do not need accounts to view information made available on most BEP's social media websites and applications. However, users must have accounts to use all the features associated with the websites and applications tailored to these specific websites and applications. This type of social media includes, but is not limited to, Facebook and Twitter;

2) Third-party applications and websites that disseminate video and image content. These social media websites and applications include, but are not limited to, YouTube. For this type of social media website or application, BEP's social media administrators must have a BEP account to post information to make it available to the public. Public users of these accounts typically do not need an account to see video on websites and applications. For public users to comment on BEP accounts (when BEP has not disabled the comment function), the public user may need an account in the website or application;

3) Third-party applications and websites that facilitate data and document sharing and repositories providing collaboration, dialogue, interaction, creation, organize, edit, comment on, combine, and share content (including Personally Identifiable Information (PII)) with entities that conduct business with BEP.)

---

[1] Transparency and Open Government Memorandum for the Heads of Executive Departments and Agencies https://www.whitehouse.gov/the_press_office/TransparencyandOpenGovernment

[2] OMB Memorandum M-10-06, *Open Government Directive* (December 8, 2009), *available at*: https://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-06.pdf

[3] OMB Circular No. A-108, Federal Agency Responsibility for Review, Reporting and Publication under the Privacy Act, *available at:* https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/circulars/A108/omb_circular_a-108.pdf.

[4] BEP Circular 40.00-14, Social Media Policy,*(December 20, 2016)*

[5] While all of social media websites facilitate two-way interactions with the public; there are some sites that BEP has decided only to conduct unilateral interactions with the public, by disabling features such as the comment feature. These interactions are covered by the Department of the Treasury Privacy and Civil Liberties Impact Assessment for the Department-wide Use of Third-Party Social Media Websites for Public Engagement, *available at*: https://www.treasury.gov/privacy/PIAs/Documents/Department%20of%20the%20Treasury%20Social%20Media.pdf.

4) Third-party applications and websites that (1) do not use web measurement and customization technologies on behalf of the BEP and (2) do not share Personally Identifiable Information (PII), or any information that could be used to determine an individual's online activity derived from such uses, with the BEP. These applications and websites are covered by different legal and policy requirements.[6]

This Privacy and Civil Liberties Impact Assessment (PCLIA) sets forth the BEP's assessment concerning the privacy and civil liberties risks associated with the use of third party social media applications and websites and the mitigation strategies BEP implements to protect PII collected, used, and maintained, when authorized, in its social media accounts. This PCLIA specifically provides the following assessment regarding BEP's use of third party social media websites and applications: (1) the specific purpose of the use; (2) any PII that is likely to become available through this interaction; (3) any intended or expected use of PII collected; (4) sharing or disclosure of the PII; (5) maintenance and retention of the PII; (6) security of the PII; (7) identification and mitigation of privacy and civil liberties risks; and (8) compliance with privacy and civil liberties requirements and other legal and policy requirements that support privacy.

In accordance with OMB Memorandum M-10-23, *Guidance for Agency Use of Third-Party Websites*,[7] BEP is required to conduct a PCLIA because the use of third party social media websites and applications makes PII available to the agency.

Section 2: Definitions

Make PII Available. The term "make PII available" includes any agency action that causes PII to become available or accessible to the agency, whether or not the agency solicits or collects it. In general, an individual can make PII available to an agency when he or she provides, submits, communicates, links, posts, or associates PII while using the website or application. "Associate" can include activities commonly referred to as "friending," "following," "liking," joining a "group," becoming a "fan," and comparable functions.

Personally Identifiable Information (PII). The term PII refers to information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. Because there are many different types of information that can be used to distinguish or trace an individual's identity, the term PII is necessarily broad. To determine whether information is PII, the agency shall perform an assessment of the specific risk that an individual can be identified using the information with other information that is linked or linkable to the individual. In performing this assessment, it is important to recognize that information that is not PII can become PII whenever additional information becomes available -in any medium or from any source -that would make it possible to

[6] OMB Memorandum M-10-22, *Guidance for Online Use of Web Measurement and Customization Technologies*, (June 25, 2010), available at: https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/memoranda_2010/m10-22.pdf.

[7] OMB Memorandum M-10-23, *Guidance for Agency Use of Third Party Websites and Applications* (June 25, 2010), *available at* http://www.whitehouse.gov/omb/assets/memoranda_2010/m10-23.pdf.

identify an individual.[8]

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 legislative, 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.

Privacy Policy. The term "privacy policy" is described in OMB M-99-18, *Privacy Policies on Federal Web Sites*[9]. This term refers to a single, centrally located statement that is accessible from an agency's official homepage. The privacy policy should be a consolidated explanation of the agency's general privacy-related practices that pertain to its official website and its other online activities.

Social media websites. For purposes of this notice, this term refers to non-governmental; third-party owned and operated websites, applications, and web-based tools (some that may be embedded on the social media website by the third-party owner of the site) that allow the creation, exchange and tracking of user-generated content. Through social media, people or groups can engage in dialogue, interact, and create, organize, edit, comment on, combine, and share content. BEP currently maintains an official presence on the following social media websites: Facebook, Twitter, and YouTube (each described in more detail in the Department of the Treasury Privacy and Civil Liberties Impact Assessment for the Department-wide Use of Third-Party Social Media Websites for Public Engagement referenced above).

Section 3: Overview

3.1: Scope

This PCLIA covers BEP's use of the Box Content Management/Enterprise Cloud Content Collaboration Platform ("Box.com"). Box.com is a third-party website that allows users to interact with a software over to the Internet to facilitate data and document sharing and collaboration stored in a cloud-based repository infrastructure. Box.com is approved by the General Services Administration (GSA) Federal Risk and Authorization Management Program (FedRAMP).

BEP will use Box.com to allow stakeholders access to BEP's data pertaining to (1) manufacturing processes, currency design and security, research and development, (2) environmental health and energy-related regulatory matters, and (2) human resource management and background

[8] OMB Memorandum M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information* (January 3, 2017), *available at:* https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2017/m-17-12_0.pdf.

[9] OMB Memorandum M-99-18, *available at:* https://www.whitehouse.gov/omb/memoranda_m99-18/

investigations matters regarding BEP contractors only.

BEP stakeholders using Box.com are:

1) Board of Governors of the Federal Reserve Board
2) Federal Reserve Banks
3) Department of Energy
4) Currency/Banknote Security Stakeholders (e.g. SIPCA Corp)
5) Currency/Banknote Paper Suppliers (e.g. Crane & Co.)
6) Federal and Local Environmental Health and/or Energy Regulators/Inspectors (e.g. U.S. Department of Energy, District of Columbia Government Department of Energy and Environment)

Box.com allows authorized and authenticated users by BEP the ability to create and/or post content in the form of data or documents in a secure cloud-based repository of folders that can be shared with other authorized users. In this instance, BEP may develop contact lists and/or contact information in order to communicate with and/or manage accounts for these users. Box.com also allows BEP's Contracting Officer Representatives (CORs) to transmit PII associated with onboarding and/or departing contractors that is used to grant access to BEP IT systems or facilities. In addition, CORs serve as intermediaries between BEP, the contractor's manager, the contractor, and the U. S. Office of Personnel Management (OPM) to complete the Electronic Questionnaires for Investigations Processing (e-QIP) system. Box.com does not interface with other BEP systems, including e-QIP, or stores users PII, but exchanges the content in the form of data or documents between BEP and authorized and authenticated users in free text fields or attached documents. The use of Box.com mitigates the need for BEP to transmit PII in BEP emails through BEP email system.

Box.com's primarily workflow process stems from the sharing of "folders." BEP Group Administrators may create a "Main-Folder," which may include sub-folders. Users are considered "Content Creators" and upon receiving access to the folder, may create, upload, download, read files, and share content contained in the folder with other authorized users. All shared files and folders are encrypted during transmission. Users may receive automated email notifications announcing the folders arrival. If the user is authorized to view the folder, they may access it through their Box.com account.

3.2 Authority to Collect

Executive Order (E.O.) 13571, Streamlining Service Delivery and Improving Customer Service,[10] sets forth requirements for government agencies using technology to improve customer service to members of the public. Section 2 of the E.O. directs agencies to: (a) establish one major initiative that will use technology to improve the customer experience; and (b) establish mechanisms to solicit customer feedback on government services and use such feedback regularly to make service improvements. This E.O. grants BEP the authority to use technology to engage with the public through the use of social media.

Section 4: Information Collection

[10] E.O.13571, Streamlining Service Delivery and Improving Customer Service, April 27, 2011. For more information, please visit: https://www.whitehouse.gov/the-press-office/2011/04/27/executive-order-13571-streamlining-service-delivery-and-improving-custom

4.1 Information Made Available vs. Information Collected

Information Likely to Become Available to BEP through Public Use of BEP Third-Party Social Media Websites

Information Made Available During the Registration Process:

Prospective Box.com users (third-party stakeholders and contractor representatives) seeking to collaborate through the Box.com website will submit their name, business entity name, phone number and email address to a BEP Trusted Agent that will submit the information to a BEP Identity Management Point of Contac ("IDM POC"). The IDM POC will verify the user's identity and authorization to interact with BEP through Box.com. BEP users seeking accounts will submit their name, email address, office name, and phone number directly to the IDM POC. The IDM POC will establish an account via the Box.com web-based access page by using the individual's name and email address. The user will establish their own password within Box.com. The IDM POC and BEP system administrators will manage user accounts and grant access to begin collaborations, secure file sharing, and content management activities with the appropriate BEP users and stakeholder(s). Users may also employ a "single sign-on" capability to enhance future accessibility.

Sources of the PII and the Method and Manner of Collection

Registered Box.com users seeking to collaborate with BEP will receive access from the IDM POC and log into the website using their name and email address (and password until they establish single sign-on access). Once web-based collaborations begin, BEP will collect PII listed below from the following individuals in order to collaborate on currency production, security, design, research and development, environmental health and energy-related regulatory matters, or to facilitate background investigations on onboarding contractors:

Stakeholder	Contractor (via Corporate Managers)	Vendors	BEP Users
• Name • Name of Entity • Business Address • Business/Mobile • Phone Number • Email Address • User Name Collected by Box.com • User Name • Email/Login ID • Password • IP Address	• Name • Company/ Corporate Entity • Date of Birth • Social Security Number (SSN) • Driver's License Number • Business/Home Address • Business/Home, and/or Mobile Phone Number • Email Address • User Name Collected by Box.com	• Name • Company/ Corporate Entity • Business Address • Business/Mobile Phone Number • Email Address • User Name Collected by Box.com • User Name • Email/Login ID • Password • IP Address	• User Name • Email/Login ID • Password • IP Address • Access Group Name • Metadata/User Access Statistical Information Collected by Box.com • User Name • Email/Login ID • Password • IP Address

	• User Name • Email/Login ID • Password • IP Address		
Manner in which information is acquired from source by the BEP project/system: (select all that apply):	**Manner in which information is acquired from source by the BEP project/system: (select all that apply):**	**Manner in which information is acquired from source by the BEP project/system: (select all that apply):**	**Manner in which information is acquired from source by the BEP 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	☐ From a paper or electronic form provided to individuals, the public or members of a particular group
Please identify the form name (or description) and/or number (e.g., OMB Control Number): _____	Please identify the form name (or description) and/or number (e.g., OMB Control Number): _____	Please identify the form name (or description) and/or number (e.g., OMB Control Number): _____	Please identify the form name (or description) and/or number (e.g., OMB Control Number): _____
☐ Received in paper format other than a form.	☐ Received in paper format other than a form.	☐ Received in paper format other than a form.	☐ 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.	☐ 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	☒ Accessed and downloaded or otherwise acquired via the internet
☐ Email	☐ Email	☐ Email	☐ Email
☐ Scanned documents uploaded to the system.	☐ Scanned documents uploaded to the system.	☐ Scanned documents uploaded to the system.	☐ Scanned documents uploaded to the system.

☐ Bulk transfer	☐ Bulk transfer	☐ Bulk transfer	☐ Bulk transfer
☐ Extracted from particular technology (e.g., radio frequency identification data (RFID) devices, video or photographic cameras, biometric collection devices).	☐ Extracted from particular technology (e.g., radio frequency identification data (RFID) devices, video or photographic cameras, biometric collection devices).	☐ Extracted from particular technology (e.g., radio frequency identification data (RFID) devices, video or photographic cameras, biometric collection devices).	☐ Extracted from particular technology (e.g., radio frequency identification data (RFID) devices, video or photographic cameras, biometric collection devices).
☐ Fax	☐ 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	☐ Extracted from notes of a phone interview or face to face contact
☒ Other: Please describe: Contact information collected in free text fields.	☒ Other: Please describe: Contact information and background investigation-related PII collected in free text fields.	☒ Other: Please describe: Contact and facility access information collected in free text fields.	☐ Other: Please describe: _____

4.2 Relevant and Necessary

The Privacy Act of 1974 requires that every federal agency, "maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required by statute or by Executive order of the President."[11] The Privacy Act allows federal agencies to exempt certain records from this requirement if certain conditions are met. This includes issuing a Notice of Proposed Rulemaking (NPRM) to solicit public opinions on the proposed exemption and issuing a Final Rule after addressing any concerns raised by the public in response to the NPRM. It is possible for some, but not all, of the information used in a system or project to be exempted from the Privacy Act through the NPRM/Final Rule process.

BEP determined that all of the PII maintained in or transmitted by Box.com is part of a series of Agency-wide, Treasury-wide, and BEP systems of records. BEP users will retrieve information by a personal identifier in order to manage contact lists and/or contact information on individuals. CORs will retrieve data in relation to background investigation processing of onboarding contractors. System Administrators will retrieve information on specific users to manage accounts and access to data. BEP is collecting the minimum amount of information necessary to support its interaction with the public on Box.com. BEP also used the processes to assess the PII to ensure that it only collects the minimal amount necessarily to allow BEP and third parties to access the website/application and collaborate on projects pertaining to BEP.

[11] 5 U.S.C. § 552a(e)(1).

4.3 Information Collection Risks and Mitigations

1) **There is a risk that BEP will collect more information than is necessary to carry out its third-party and social media website purposes.**

   BEP mitigates this risk by determining whether information is relevant and necessary to a BEP mission before collecting any PII on Box.com. Box.com involves the collection of PII for the purposes described in Section 4.1 above. BEP continuously reviews its collection of PII for Box.com purposes to mitigate the risk of collecting more information than is necessary to carry out its mission-related purposes.

   BEP also does not use Box.com to monitor users. BEP provides the Box.com users with alternatives to seeking information or submitting questions. The Box.com users can obtain comparable information and services by (1) visiting BEP's website at www.bep.gov or www.moneyfactory.gov; (2) calling BEP at 1-877-874-4114 (toll- free) or (202) 874-4000; or (3) emailing at moneyfactory.info@bep.gov.

2) **There is a risk that the individuals will not know what privacy policy or notice applies to the collection of their information.**

   BEP mitigates this risk by providing a Privacy Act Notice for Trusted Agents to present to users requesting access prior to soliciting PII to facilitate access. BEP will also provide a banner on the Box.com website that informs users that they are subject to the privacy policies associated with the third-party website. To further mitigate this risk, BEP will add the Privacy Act Notice to the page containing free text fields that will be used to collect PII for authorized BEP uses.

   By using the Box.com website, users are subject to data collection pertaining to usage, logs, device information, and cookie and statistical tracking technologies. Box.com uses this information that includes, but not limited to:

   - Provide, operate, maintain and improve Box.com services;
   - Enable access and use of Box.com services, including uploading, downloading, collaborating on, sharing content, and sending emails the user's behalf;
   - To send technical notices, updates, security alerts and support, and administrative messages;
   - Provide and deliver user-requested services, process and complete transactions; and
   - Respond to your comments, questions, and requests and provide customer service and support.

3) **There is a risk that individuals who visit BEP third-party social medial websites will not know about embedded links/applications on the social media website**.

   BEP provides notice to users who visit official BEP owned and operated websites (as opposed to BEP pages on third-party social media) when the website embeds a link to a social media website or application on the webpage. Visitors who select these links are also warned that they should review the privacy policy of the site to which they are being redirected. These policies further explain the effects of using links on BEP owned and

operated websites and navigating to non-government websites.

Box.com (including service providers working on their behalf) use various technologies to collect information, which may include saving cookies to an individual's computer or mobile device. Cookies are small data files stored on the user's hard drive or in device memory that help Box.com to improve services and the web experience, customize preferences, allow access without re-entering the password (single sign-on feature), understand which areas and features are most popular and count visits. Box.com also collect information using web beacons (also known as "tracking pixels"). Web beacons are electronic images (also called "gifs") that may be used in the Box Services or in emails that help to deliver cookies, count visits, understand usage, and determine whether an email has been opened and acted upon. Box.com provides the opportunity to disable cookies, update, correct or delete information pertaining to the user at any time by logging into their online account and modifying their information or by emailing privacy@box.com.

4) **There is a risk that individuals who do not have a social media account may not want to use social media or provide PII to engage with BEP.**

   BEP mitigates this risk by providing Box.com's users the ability to provide PII via secure email transactions or by phone. In addition, Box.com's users can learn about BEP's activities and communicate with BEP without having to go to Box.com website by visiting the Contact Us page on the BEP website.

   Unless they establish an account, however, users who wish to visit the Box.com website will not be able to use all of the functions (e.g., collaborating and sharing information) made available to registered users.

5) **There is a risk that visitors to a BEP third-party social media site will not know whether the site is an official BEP social media site.**

   This helps users understand what information Box.com collects from their interaction with the website and the purposes for which the data is collected. BEP will also place a link to the BEP homepage located at: https://www.moneyfactory.gov/privacy.html.

BEP evaluates risks before using new third-party social media websites and monitors changes to privacy policies to determine whether it needs to reevaluate the risks associated with its uses of these websites. BEP conducts these reviews to identify and mitigate risks prior to publishing a new BEP third-party social media page or continuing to use these websites.

Section 5: Maintenance, use and sharing of the information

5.1 Describe how and why the system/project uses the information it collects and maintains.

BEP limits the information that it collects through its Box.com website to:

1) **Information from BEP Third Party Stakeholders:** BEP uses this information, which

consists of user account and contact information, to manage user/access accounts and to provide contact information to BEP stakeholders collaborating on BEP activities and initiatives related to the Federal Reserve Board of Governors and the Federal Reserve Banks collaborating with BEP on currency-related processes, procedures, and policies. BEP also collects contact information in order to collaborate with Federal and Local Environmental Health and/or Energy Regulators/Inspectors (e.g. U.S. Department of Energy, District of Columbia Government Department of Energy and Environment) conducting oversite activities at BEP facilities. BEP also collects contact information from currency/banknote security and paper supply stakeholders (e.g. SIPCA Corp and Crane & Co.) conducting currency-related business or seeking access to BEP facilities.

2) **Information from Corporate Managers of BEP Contractors**: BEP uses this information to share information with the U. S. Office of Personnel Management (OPM) online e-QIP Background Investigation Process for onboarding or departing contractors.

5.2 Ensuring accuracy, completeness, and timeliness of information maintained, used and shared

The Privacy Act requires that 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."[12]

The Act only applies to records containing PII that are maintained in a "system of records." This means that the records must be maintained in an information system or paper file and then retrieved by a personal identifier. The PII maintained in this system are part of a series of "system of records" and no exemption are claimed from the accuracy, relevance, timeliness, and completeness requirements. BEP applies the fair information practice principles and works to ensure the accuracy, completeness, and timeliness of information maintained, used and shared. BEP recognizes that information is more likely to be accurate when it is derived directly from the individual. All information BEP collects from third-party or social media websites is derived from the individual or human resource representatives for onboarding contractors.

Direct Collection from Individuals When Information May Result in Adverse Determinations

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). Information derived from the individual is more likely to be accurate. BEP ensures the accuracy, relevance, completeness, and timeliness of the information it maintains or transmits in the system by collecting the information directly from the individual strategic partner or vendor. In certain instances, the information is collected from corporate representatives that receive the information directly from onboarding contractors. Since the corporate representative collects the PII directly from the individual to whom it pertains, the risk of collecting inaccurate information is minimized.

[12] 5 U.S.C. § 552a.(e)(5).

BEP assumes that the individual providing the information is the account holder identified in the account name for the person providing the information, but recognizes that social media accounts are sometimes used by third-parties with or without the consent of the account holder. The BEP Office of Security has procedures in place to communicate directly with onboarding or departing contractors that submit PII associated with the OPM e-QIP Background Investigation process prior to making any adverse determinations about an individual's rights, benefits, and privileges under federal programs based on information collected from third-party social media. Visitors to BEPs third-party webpages may, however, be subject to the third-party website's rules as stated in its privacy and usage policy over which BEP has no control.

Ensuring Fairness in Making Determinations about Individuals

Under the Privacy Act, all 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."[13]

BEP extracts information from Box.com and retains the information in the same form in which it was provided by the individual on the webpage. The individual who is the subject of the information provided it directly to the BEP webpage or other social media platform. Therefore, BEP assumes the accuracy of the information.

5. 3 Information sharing within the Department of the Treasury

Internal Information Sharing

PII derived from Box.com is only shared with those BEP employees and contractors who have a need for the PII in the performance of their duties.

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

External Information Sharing

Third-Party Social Media Pages: BEP may share information it receives from the Box.com website in accordance with the Privacy Act, 5 U.S.C. 552a or the Routine Uses of the Privacy Act System of Records for which the data was retrieved. BEP may also share the information collected with the National Archives and Records Administration (NARA) in compliance with Federal Records Act requirements, or in response to NARA Office of Government Information Services requests relating to BEP compliance with the Freedom of Information Act. BEP may also share the information with contractors to compile, organize, analyze, program, or otherwise refine the information to accomplish an agency function. BEP may also share the information with a Congressional office in response to an inquiry made at the request of the individual to whom the information pertains. If BEP suspects or confirms a compromise of the security or confidentiality of PII posted on a BEP owned and operated website, BEP will share the information with appropriate agencies, entities, and persons when reasonably necessary to assist in connection with the Department's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm. BEP may also share the information with the Department of

[13] Section 552a(e)(5)

Justice for investigation, legal advice and/or representation.

Section 6: Legal 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 and how BEP mitigates those risks: (1) The Privacy Act of 1974 System of Records Notice Requirement; (2) the Paperwork Reduction Act; (3) the Federal Records Act; (4) the E-Government Act of 2002 security requirements; and (5) Section 508 of the Rehabilitation Act of 1973.

6.1 Privacy Act System of Records Notice (SORN)

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

Compliance with the SORN Requirement

BEP determined that the information it collects and maintains from Box.com is subject to the Privacy Act because information is retrieved by personal identifier. The following SORNS apply:

Treasury .015 - General Information Technology Access Account Records – Provides coverage for all users (members of the public and BEP employees and contractors) who are authorized to access Treasury information technology resources in furtherance of a BEP mission.

Treasury .017 - Correspondence and Contact Information – Provides coverage for all persons submitting contact information to BEP to initiate collaboration or information sharing related to a BEP mission.

Treasury/BEP .021 - Investigative Files – Provides coverage for data submitted by managers of onboarding or departing contractors.

Treasury/BEP .027 - Access Control and Alarm Monitoring Systems (ACAMS) – Provides coverage for BEP stakeholders seeking access to BEP facilities in furtherance of a BEP mission.

6.2 The Paperwork Reduction Act

The Paperwork Reduction Act (PRA) requires OMB approval before a federal agency may collect standardized (i.e., the same) data from 10 or more respondents within a 12 month period.

Compliance with the PRA Requirement

As described above, BEP's use of Box.com is not subject to the provisions of the Paperwork Reduction Act (PRA), 44 U.S.C. § 3401 *et. seq*. as BEP will not be collecting information in such a manner as to trigger the PRA. Box.com will not serve as the primary repository for BEP data. It operates in conjunction with information currently maintained in other BEP systems and/or activities associated with Contractor vetting. There are no forms associated with Box.com transmissions or data collections. The remaining information pertains to user contact information or data pertaining to the subject matter associated with strategic currency-related initiatives, (e.g. currency design, research and development). Should a BEP user elect to use the system in a manner that would require the collection of information from 10 or more persons by means of identical questions or identical reporting, recordkeeping, or disclosure requirements within the same 12 month period, then the specific vehicle (i.e. form, survey, questionnaire) used to solicit that information would need to evaluated under the PRA. However, the use of Box.com as a

communications or storage tool does not trigger the PRA.

6.3 Records Management - NARA/Federal Records Act Requirements

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

NARA Records Retention Requirements

If PII is posted on a social media website, it may become a federal record if it is used by BEP to transact business. Most of the information that is posted by the public on BEP social media webpages via is categorized as "non-record" unless BEP performs some type of follow-up action to respond to a posted comment. For example, if BEP responds to a post by a member of the public and uses the information provided in the comment as supporting documentation for a BEP decision (white paper or BEP policy,) that post and the BEP response is a record. The retention schedule that applies to the information retained would depend upon the subject and records schedule for the BEP decision. Under these circumstances, the Department must maintain a copy according to the requirements in the applicable records retention policy (policies that determine how long BEP will retain information before destroying it or sending it to NARA for permanent archiving).

Box.com NARA-approved Records Retention Schedules are as follows:

- GRS 5.5 Mail, Printing, and Telecommunication Service Management Records,
  Item 020- DAA-GRS-2016-0012-0002 – Mail, printing, and telecommunication services control records. Temporary. Destroy when 1 year old or when superseded or obsolete, whichever is applicable, but longer retention is authorized if required for business use.

- GRS 5.6 Security Records, Item 180 and 181, Personnel Security and Access Clearance Records.
  Item 180- DAA-GRS-2017-0006-0024 - Temporary. Destroy 1 year after consideration of the candidate ends, but longer retention is authorized if required for business use.

  Item 181- DAA-GRS-2017-0006-0025 - Temporary. Destroy 5 years after employee or contractor relationship ends, but longer retention is authorized if required for business use.

- BEP 70 Series – Currency Production Records (N1-3180-4-20 & N1-318-09-01)
  70.1 Currency Printing & Processing N1-3180-4-20
  Item 1.a. Annual Currency Orders Permanent - Cut off files at end of each fiscal year and transfer to the BEP's records storage area when volume warrants or when 5 years old. Transfer to NARA in five year blocks when the most recent record is 25 years old.

  70.3 Securities Technology Research & Testing N1-318-06-01,
  Item 1.c. (1. & 3.) Research and testing, Lab Tests Monitoring Equipment and Materials
  1. Calibration and Verification of Equipment Temporary. Cut off files after the last entry in the log book. Transfer to BEP's records storage area. Destroy when the last entry in the log book is 2 years old.
  3. Reports on Test Results (generated from Items 1 and 2) Temporary. Cut off files at end of each fiscal year. Transfer to BEP's records storage area when 2 years old. Destroy when

7 years old.

- BEP 80 Series – BEP Information Technology Operations, Services, and Records (N1-318-04-2)

  80.1 Information Systems- N1-318-04-02

  Item 1. (a. & b.) Bureau of Engraving and Printing Management Information System (BEPMIS).

  a. Electronic data - Permanent. Transfer to NARA when 30 years old.

  b. All other files - Temporary. Close out files at end of each fiscal year. Hold in office at least 7 years, then delete when no longer needed.

6.4 E-Government Act/NIST Compliance

The completion of Federal Information Security Modernization Act (FISMA) Security Assessment & Authorization process is required before a federal information system may receive Authority to Operate.

Federal Information System Subject to FISMA/ Security Assessment and Authorization

Box.com is subject to federal IT Security requirements under the Federal Information Security Modernization Act[14] ("FISMA"), which mandates that it undergo a Security Assessment & Authorization (SA&A), which leads to a federal information system receiving an Authority to Operate ("ATO"). Box.com is also subject to stringent federal policies and mandates associated with third-party websites and digital services. Box.com ensures encryption of BEP data at rest and in transit. Security policies set within Box.com mitigate accidental leaks, prevents automatic deletion of files, and enforce data centralization. Box.com meets FedRAMP compliance by ensuring that security controls are tailored to meet BEP's operational needs. Box.com uses baseline physical and logical access protections for all data in its environment.

Additionally, user accounts to login to Box.com must be approved and implemented through BEP's Identity Management (IDM) process. User accounts are only issued to authorized BEP employees or contractors, or verified and authenticated users operating under a BEP executed agreement with suitable Non-Disclosure Agreements (NDA) and information protection clauses; Users are assigned role-based access controls by Folder Owners folders within the environment which limit their access rights and functions they are permitted to perform on files/folders (e.g., read-only, read-write, etc.)

Certain folders may be designed to store sensitive PII temporarily as a secure mechanism to send the information to BEP (e.g., Contractor PII information for support background clearances). These folders will have the same limited access controls. Files uploaded to these folders will be transferred to the internal BEP system of record and removed from the Box.com platform.

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

[14] Federal Information Security Modernization Act, Pub. L. 113-283 (December 18, 2014), *available at*: https://www.gpo.gov/fdsys/pkg/PLAW-113publ283/pdf/PLAW-113publ283.pdf

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.

Compliance with Section 508 of the Rehabilitation Act of 1973

Box.com submitted a Voluntary Product Accessibility Template (VPAT) assessment document that reflects Section 508 Compliance features and capabilities available to its users, *available at*: https://accessibility.ua.edu/vpat/vpat_box.pdf).

In addition, BEP provides alternative 508 compliant sites where individuals with disabilities may access general information or methods to contact appropriate BEP stakeholders outside of the Box.com platform. This alternative site is located on: http://www.moneyfactory.gov/.

Section 7: Redress

7.1 Access under the Freedom of Information Act and Privacy Act

Individuals seeking records created in Box.com and maintained by BEP may file a Freedom of Information Act and/or Privacy Act request with BEP's Privacy Act Officer in accordance with 31 C.F.R. Part 1.

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
Michael J. Pease
Chief, Office of Critical Infrastructure and IT Security
Bureau of Engraving and Printing
Department of the Treasury

Approval Signature

//S// (mm/dd/yy)

_____

Michael J. Pease
Chief, Office of Critical Infrastructure and IT Security