Affects Members Of the Public? □

## Department of Energy

# Privacy Impact Assessment (PIA)

***Guidance is provided in the template. See DOE Order 206.1, Department of Energy Privacy Program, Appendix A, Privacy Impact Assessments, for requirements and additional guidance for conducting a PIA: https://www.directives.doe.gov/directives-documents/200-series/0206.1-BOrder/@@images/file***

**Please complete form and return via email to Privacy@hq.doe.gov**

**No hand-written submissions will be accepted.**

**This template may not be modified.**

## MODULE I – PRIVACY NEEDS ASSESSMENT

| | | |
|---|---|---|
| **Date** | August 19, 2019 | |
| **Departmental Element & Site** | OCIO IM-60 | |
| **Name of Information System or IT Project** | Box Enterprise Cloud Content Collaboration Platform | |
| **Exhibit Project UID** | TBD | |
| **New PIA** X<br>**Update** □ | New PNA/PIA | |
| | **Name, Title** | **Contact Information Phone, Email** |
| **System Owner** | Mark Gold | 19901 Germantown Rd<br>Germantown, MD 20874<br>202-695-9185<br>Mark.Gold@hq.doe.gov |

## MODULE I – PRIVACY NEEDS ASSESSMENT

| | | |
|---|---|---|
| **Local Privacy Act Officer** | Ken Hunt | 1000 Independence Avenue, S.W.<br>Washington D.C 20585<br>202-586-8695<br>Ken.hunt@hq.doe.gov |
| **Cyber Security Expert** reviewing this document (e.g. ISSM, CSSM, ISSO, etc.) | Jacquelyn Bell | 19901 Germantown Rd<br>Germantown, MD 20874<br>(301) 903-7114<br>Jacquelyn.Bell@hq.doe.gov |
| **Person Completing this Document** | Mark Gold | 19901 Germantown Rd<br>Germantown, MD 20874<br>202-695-9185<br>Mark.Gold@hq.doe.gov |
| **Purpose of Information System or IT Project** | The Box Enterprise Cloud Content Collaboration Platform (Box) provides a secure way to share content and improve collaboration on any device. Box offers a platform for file synchronization and sharing for a more effective collaboration across devices, teams and organizations. Box provides secure content management and collaboration capabilities to customized web and mobile apps without having to build or maintain a separate content layer.<br>The DOE Office of Public Affairs (PA) intends to use Box to: (1) facilitate the transfer of large files, including video files, to both internal and external recipients; (2) manage and transmit information content, such as newsletters; and (3) facilitate digital asset management, including the ability to tag, collaborate, and share large multimedia files.<br>□<br>□<br>□ | |
| **Type of Information Collected or Maintained by the System**: | □<br>□ SSN Social Security number<br>□ Medical & Health Information e.g. blood test results<br>□ Financial Information e.g. credit card number<br>□ Clearance Information e.g. "Q"<br>□ Biometric Information e.g. finger print, retinal scan<br>□ Mother's Maiden Name | |

| | |
|---|---|
| | DoB, Place of Birth<br>Employment Information<br>Criminal History |

## MODULE I – PRIVACY NEEDS ASSESSMENT

| | |
|---|---|
| | □ Name, Phone, Address<br>☒ Other – Please Specify<br>*TBD \| Requirements are being developed for the following information*:<br>• Video Management (i.e. Speaking Engagement(s), Conference(s), etc.)<br>• "Public Domain" information (i.e. Energy News, Energy Blog, etc.)<br>• DOE Lab, field location(s), Assessment information (stored temporarily until assessment is complete). |
| **Has there been any attempt to verify PII does not exist on the system?**<br>**DOE Order 206.1, *Department of Energy Privacy Program,* defines PII as** *any information collected or maintained by the Department about an individual, including but not limited to, education, financial transactions, medical history and criminal or employment history, and information that can be used to distinguish or trace an individual's identity, such as his/her name, Social Security number, date and place of birth, mother's maiden name, biometric data, and including any other personal information that is linked or linkable to a specific individual.* | N/A |
| **If "Yes," what method was used to verify the system did not contain PII? (e.g. system scan)** | N/A |

## Threshold Questions

| | |
|---|---|
| **1. Does system contain (collect and/or maintain), or plan to contain any information about individuals?** | No |

## MODULE I – PRIVACY NEEDS ASSESSMENT

| | |
|---|---|
| **2. Is the information in identifiable form?** | No |
| **3. Is the information about individual Members of the Public?** | No |
| **4. Is the information about DOE or contractor employees?** | No |

If the answer to **all** four (4) Threshold Questions is "**No**," you may **proceed to the signature page** of the PIA. Submit the completed PNA with signature page to the CPO.

**Module II must be completed for all systems if the answer to any of the four (4) threshold questions is "Yes." All questions must be completed. If appropriate, an answer of N/A may be entered.**

The goal of the threshold questions is to legitimately and efficiently determine whether additional assessment is necessary. If there is doubt, it is in the System Owner's best interest to complete Module II.

PIAs affecting Members of the Public are posted on the DOE Privacy website. For this reason, PIAs affecting Members of the Public should be written in plain language and at a high level so they are easily understandable and do not disclose sensitive information.

## END OF PRIVACY NEEDS ASSESSMENT

## MODULE II – PII SYSTEMS & PROJECTS

### AUTHORITY, IMPACT & NOTICE

| MODULE II – PII SYSTEMS & PROJECTS | |
|---|---|
| **1. AUTHORITY**<br>**What specific authorities authorize this system or project, and the associated collection, use, and/or retention of personal information?** | • Department of Energy Authorization Act, Title 42, United States Code (U.S.C), Section 7101 *et. seq*.,<br>• 50 U.S.C. 2401 *et. seq*. |
| **2. CONSENT**<br>**What opportunities do individuals have to decline to provide information (e.g. where providing information is voluntary) or to consent only to particular uses of the information (other than required or authorized uses)?** | No voluntary submission or mandatory collection of information is performed. All identifiable information is collected from other DOE systems. Box performs Identification and Authentication within Active Directory. There is no use of the information other than required or authorized use.<br>The Box Enterprise Cloud Content Collaboration Platform is only accessible to credentialed users within the DOE network. All systems on the network display a warning banner as required by DOE 0 205.1B, paragraph 4.c (11), which directs that SDM Risk Management Implementation Plans "Must require DOE and NNSA NSS and Federal unclassified systems to display a system use notification (e.g. Warning Banner) at login and require users to electronically acknowledge the warning (such as clicking on 'OK' or 'I agree' button to proceed)." |
| **3. CONTRACTS**<br>**Are contractors involved with the design, development and maintenance of the system? If yes, was the Privacy Order CRD or Privacy Act clauses included in their contracts?** | Contractors are involved with the design, development and maintenance of the system.<br>Yes. |
| **4. IMPACT ANALYSIS:**<br>**How does this project or information system impact privacy?** | Box transmits documents and videos that may contain PII. Those files are not maintained by the Box system. |

## MODULE II – PII SYSTEMS & PROJECTS

| | |
|---|---|
| **5. SORNs**<br>**How will the data be retrieved? Can PII be retrieved by an identifier (e.g. name, unique number or symbol)?**<br>**If yes, explain, and list the identifiers that will be used to retrieve information on the individual.** | N/A |
| **6. SORNs**<br>**Has a Privacy Act System of Records Notice (SORN) been published in the *Federal Register*?**<br>**If "Yes," provide name of SORN and location in the *Federal Register*.** | N/A |
| **7. SORNs**<br>**If the information system is being modified, will the SORN(s) require amendment or revision?** | N/A |
| **DATA SOURCES** | |
| **8. What are the sources of information about individuals in the information system or project?** | Files and videos are uploaded into Box by authorized DOE Public Affairs and DOE site staff. Documents and videos are official DOE media records. |
| **9. Will the information system derive new or meta data about an individual from the information collected?** | N/A- Box does not allow for the identification of individuals. |
| **10. Are the data elements described in detail and documented?** | N/A |

## MODULE II – PII SYSTEMS & PROJECTS

| | |
|---|---|
| **DATA USE** | |
| **11. How will the PII be used?** | Active Directory credentials of users enables authorized users to upload documents and media into Box. Documents and videos may include images and names of individuals speaking in their official business capacities. |
| **12. If the system derives meta data, how will the new or meta data be used?**<br>**Will the new or meta data be part of an individual's record?** | N/A |
| **13. With what other agencies or entities will an individual's information be shared?** | Box is only used to transmit files and videos between authorized DOE users. i |
| **REPORTS** | |
| **14. What kinds of reports are produced about individuals or contain an individual's data?** | N/A |
| **15. What will be the use of these reports?** | N/A |
| **16. Who will have access to these reports?** | N/A |
| **MONITORING** | |

| MODULE II – PII SYSTEMS & PROJECTS | |
|---|---|
| **17. Will this information system provide the capability to identify, locate, and monitor individuals?** | NA. |
| **18. What kinds of information are collected as a function of the monitoring of individuals?** | NA |
| **19. Are controls implemented to prevent unauthorized monitoring of individuals?** | Box ensures session authenticity through protocols as all external web connections are directed to use https using TLS 1.2.<br>Box has enabled HTTP strict transport Security (HSTS) and Box customer should ensure that they are using modern browsers that implement the same. The browser will forces the Box Domain.<br>Box has implemented an alternative address to manage the risk of data origin. |
| **DATA MANAGEMENT & MAINTENANCE** | |
| **20. How will records about individuals be kept current and verified for accuracy, relevance and completeness? Include PII data collected from sources other than DOE records.** | N/A- Box does not verify the accuracy or completeness of the DOE federal and contractor data in the system. This functionality is conduct by other DOE system(s)/application(s). |
| **21. If the information system is operated in more than one site, how will consistent use of the information be ensured at all sites?** | Box is a Software as a Service (SaaS) solution and can be accessed on any DOE network. The system provides a single repository containing all system information and the rules, controls, and procedures that govern access to the system will be applied consistently, regardless from which site the system is accessed. |
| **RECORDS MANAGEMENT** | |
| **22. Identify the record(s).** | TBD |

| **MODULE II – PII SYSTEMS & PROJECTS** | |
|---|---|
| **23. Identify the specific disposition authority(ies) that correspond to the record(s) noted in no. 22.** | Check appropriately and cite as required.<br>Scheduled<br>GRS 6.4<br>*All DOE records schedules are in the process of being converted to media neutral schedules. To the extent that any record in Box is covered by a DOE mission specific schedule, it may not be disposed of until the new media neutral schedule is approved by NARA. |
| **24. Records Contact** | TBD |
| **ACCESS, SAFEGUARDS & SECURITY** | |
| **25. What controls are in place to protect the data from unauthorized access, modification or use?** | Technical and administrative controls are in place to prevent the misuse of data by individuals with access. These access controls are part of the DAYS System Security Plan (SSP).<br>All system team members (Federal and contractor) are required to annually complete the Department of Energy Headquarters Annual Cyber Security Refresher Briefing as a necessary requirement for access to the system.<br>Administrative controls include separation of duties so individuals only have access to appropriate personal information, and use of system audit logs to monitor access and user activity in the system. Rules of behavior and consequences for violating the rules are displayed to the user each time the user logs onto the system.<br>The technical controls include restricted access via unique user-id and password with access/functional privileges to Box commensurate with the user's job responsibilities. |
| **26. Who will have access to PII data?** | Authorized users |
| **27. How is access to PII data determined?** | Access to data is determined by evaluation of personnel job roles and responsibilities and organization. Based on the evaluation, the user is assigned permissions that are applied using system access control lists. |

| MODULE II – PII SYSTEMS & PROJECTS | |
|---|---|
| **28. Do other information systems share data or have access to the data in the system? If yes, explain.** | No |
| **29. For connecting information systems, is there an Interconnection Security Agreement (ISA) or other agreement between System Owners to ensure the privacy of individuals is protected?** | N/A |
| **30. Who is responsible for ensuring the authorized use of personal information?** | Access to data is determined by evaluation of personnel job roles and responsibilities and organization. Based on the evaluation, the user is assigned permissions that are applied using system access control lists. |
| END OF MODULE II | |

## SIGNATURE PAGE

| | Signature | Date |
|---|---|---|
| **System Owner** | **(Print Name)**<br>**(Signature)** | |
| **Local Privacy Act Officer** | **(Print Name)**<br>BROOKE DICKSON Digitally signed by BROOKE DICKSON Date: 2019.11.21 10:55:32 -05'00'<br>**(Signature)** | |
| ***Ken Hunt***<br>**Chief Privacy Officer** | **(Print Name)**<br>WILLIAM HUNT Digitally signed by WILLIAM HUNT Date: 2019.11.21 09:29:49 -05'00'<br>**(Signature)** | |