



PRIVACY IMPACT ASSESSMENT:
Office of the Chief Information Officer – UnitySync
PIA Template Version 5 – August 2017

Affects Members Of the Public?	<input type="checkbox"/>
--------------------------------------	--------------------------

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	February 21, 2024	
Departmental Element & Site	Office of the Chief Information Officer (OCIO), Enterprise Operations & Shared Services, IM-60, Infrastructure Operations Office, IM-61, Germantown, MD	
Name of Information System or IT Project	UnitySync	
Exhibit Project UID	019-000001877	
New PIA Update	<input checked="" type="checkbox"/>	This is a new PIA for the UnitySync tool
	<input type="checkbox"/>	
	Name, Title	Contact Information Phone, Email
System Owner	Damon Bragg Information Technology Specialist Infrastructure Operations Office, IM-61	301-903-0015 damon.bragg@hq.doe.gov



PRIVACY IMPACT ASSESSMENT:
 Office of the Chief Information Officer – UnitySync
 PIA Template Version 5 – August 2017

MODULE I – PRIVACY NEEDS ASSESSMENT

Local Privacy Act Officer	Director of Privacy Management and Compliance Office of the Chief Information Officer, IM-42	privacy@hq.doe.gov
Cyber Security Expert reviewing this document (e.g. ISSM, CSSM, ISSO, etc.)	Gregory Huber Technical Point of Contact (POC), IM-61	301-903-9925 gregory.huber@hq.doe.gov
Person Completing this Document	Nancy Blazewick Information Systems Security Officer (ISSO) Security and Compliance, IM-63	757-771-2691 nancy.blazewick@hq.doe.gov
Purpose of Information System or IT Project	<p>The UnitySync runs on a web server, allowing users to administrate their syncs using a web browser. UnitySync is a centralized service that synchronizes data between email directories & databases providing a unified view in your mail client address books. Department of Energy utilizes LDAP (active directory) connectivity to populate and synchronize our Global Address List in Microsoft Outlook with contact information for users at DOE facilities nationwide. It ensures that changes made in one directory source are replicated accurately to the other connected systems, helping to maintain data integrity and consistency across both Headquarters (HQ), DOE field sites and local labs.</p> <p>The UnitySync application runs on the Windows 2016 server AVASYNDCRPR01.Sync.Local, which is hosted in Amazon Web Services (AWS). This server is also an Active Directory Domain Controller for the “sync.local” domain. There are two additional Domain Controllers, a Windows 2016 server named AVASYNDCRPR02.sync.local (hosted in AWS), and a Windows 2016 server named GTN-SYN-DCR-P01.sync.local (hosted in DOE’s Germantown datacenter). This application tool is located in the DOE EITS boundary and inherits infrastructure protections from the Common Operating Infrastructure (COI).</p>	



PRIVACY IMPACT ASSESSMENT:
Office of the Chief Information Officer – UnitySync
PIA Template Version 5 – August 2017

MODULE I – PRIVACY NEEDS ASSESSMENT

<p>Type of Information Collected or Maintained by the System:</p>	<ul style="list-style-type: none"> <input type="checkbox"/> SSN Social Security number <input type="checkbox"/> Medical & Health Information e.g. blood test results <input type="checkbox"/> Financial Information e.g. credit card number <input type="checkbox"/> Clearance Information e.g. "Q" <input type="checkbox"/> Biometric Information e.g. finger print, retinal scan <input type="checkbox"/> Mother's Maiden Name <input type="checkbox"/> DOB, Place of Birth <input type="checkbox"/> Employment Information <input type="checkbox"/> Criminal History <input checked="" type="checkbox"/> Name, Business Phone, Business Address <input checked="" type="checkbox"/> Other – UnitySync Attributes Ex Job title, Organization name, Email, Employee ID
--	--

<p>Has there been any attempt to verify PII does not exist on the system?</p> <p><i>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.</i></p>	<p>YES exists</p>
<p>If "Yes," what method was used to verify the system did not contain PII? (e.g. system scan)</p>	<p>N/A</p>

Threshold Questions



MODULE I – PRIVACY NEEDS ASSESSMENT

1. Does system contain (collect and/or maintain), or plan to contain any information about individuals?	YES
2. Is the information in identifiable form?	YES
3. Is the information about individual Members of the Public?	NO
4. Is the information about DOE or contractor employees?	<input checked="" type="checkbox"/> Federal Employees <input checked="" type="checkbox"/> Contractor Employees

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



PRIVACY IMPACT ASSESSMENT:
 Office of the Chief Information Officer – UnitySync
 PIA Template Version 5 – August 2017

MODULE II – PII SYSTEMS & PROJECTS

<p>1. AUTHORITY</p> <p>What specific authorities authorize this system or project, and the associated collection, use, and/or retention of personal information?</p>	<p>DOE O 205.1C, Department of Energy Cyber Security Program, and associated NIST SP 800-53, Rev 4, Recommended Security Controls for Federal Information Systems and Organizations, identifies controls to ensure adequate protection of CUI, including PII, and applies requirements and guidance from OMB memorandum M-06-19, Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments, pertaining to the protection of PII.</p>
<p>2. CONSENT</p> <p>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)?</p>	<p>UnitySync is only accessible from within the DOE network. Users consent by logging on to the system. Consent is required for access to tools used for business functions. A limited amount of credentialing is pulled from Active Directory (AD).</p> <p>PII data such as name, phone telephone number, and organization name are manually provided by users in GAL upon onboarding.</p>
<p>3. CONTRACTS</p> <p>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?</p>	<p>Contractors are involved with the design, development, and maintenance of the system.</p> <p>The individuals providing this type of information are subject to the same limitations applicable to DOE officers and employees under the Privacy Act, 5 U.S.C. 552a.</p> <p>Yes. Contract clauses require the contractors to safeguard all information that they may obtain in accordance with the provisions of the Privacy Act and the requirements of the DOE.</p>



MODULE II – PII SYSTEMS & PROJECTS

<p>4. IMPACT ANALYSIS:</p> <p>How does this project or information system impact privacy?</p>	<p>UnitySync application uses information already available through Active Directory, etc. PII attributes processed by the system are considered non sensitive in nature neither can they be aggregated to create new sensitive PII data. PII data processed by the system are limited to Official Email, Office Location, Primary / Mobile Phone Number.</p> <p>UnitySync application is limited to DOE/OCIO users where request for access is determined by System Owner and/or System Administrator. To be granted any of the System Roles for the UnitySync application, a user must first meet the following access requirements to be added to any environment:</p> <ul style="list-style-type: none"> • Enabled in Active Directory (AD) • Has an active license • Member of the environment’s security group <p>UnitySync application is not the authoritative source for the privacy data stored within its system environment and thus, impact to privacy should be considered low. The focus of UnitySync is to allow synchronization for both HQ and DOE-ID email customers to locate each DOE Site’s and Labs for up-to-date published contacts in each respective Global Address List (GAL). The following attributes are amongst those collected by the system considered to be some variation of PII:</p> <p>Name, Title, Mobile number, Employee ID, Department, Street Address, Proxy Addresses, Display name, other telephone, Instance Type, Home page, Street address</p>
<p>5. SORNs</p> <p>How will the data be retrieved? Can PII be retrieved by an identifier (e.g. name, unique number or symbol)?</p> <p>If yes, explain, and list the identifiers that will be used to retrieve information on the individual.</p>	<p>Data can be retrieved by logging into the system with sign in credentials and syncing via Local Active Directory by Name, Location, Extension, or by organization/company name.</p> <p>Data and site owners would be responsible for this administration of their SORN.</p>



PRIVACY IMPACT ASSESSMENT:
 Office of the Chief Information Officer – UnitySync
 PIA Template Version 5 – August 2017

MODULE II – PII SYSTEMS & PROJECTS

6. SORNs Has a Privacy Act System of Records Notice (SORN) been published in the <i>Federal Register</i> ? If "Yes," provide name of SORN and location in the <i>Federal Register</i> .	NO
7. SORNs If the information system is being modified, will the SORN(s) require amendment or revision?	NO
DATA SOURCES	
8. What are the sources of information about individuals in the information system or project?	<ul style="list-style-type: none"> DOE Outlook contacts. A limited amount of credentialing is pulled from Local Active Directory
9. Will the information system derive new or meta data about an individual from the information collected?	No, the system does not and will not derive new meta data considered to be PII about an individual from the information collected.
10. Are the data elements described in detail and documented?	NO
DATA USE	
11. How will the PII be used?	<p>The use of UnitySync application is for the DOE staff and various other field sites for customer to use.</p> <p>Low level of PII is used to control access to the system-by-system administrators, but not use to control access to contacting individuals.</p>



PRIVACY IMPACT ASSESSMENT:
Office of the Chief Information Officer – UnitySync
PIA Template Version 5 – August 2017

MODULE II – PII SYSTEMS & PROJECTS

<p>12. If the system derives meta data, how will the new or meta data be used?</p> <p>Will the new or meta data be part of an individual's record?</p>	Not applicable
<p>13. With what other agencies or entities will an individual's information be shared?</p>	None
Reports	
<p>14. What kinds of reports are produced about individuals or contain an individual's data?</p>	Reports are generated for the administration of the system and may contain information about user accounts. Users can export Excel files of the contact and organization data containing data elements outlined in question 4.
<p>15. What will be the use of these reports?</p>	Reports will be used for administrative purposes including support of system content administration and security.
<p>16. Who will have access to these reports?</p>	<p>Only authorized DOE federal and contractor personnel with elevated privileges will have access to these reports. Furthermore, only administrators whose role and function correspond with the data contained in the report will be able to access said reports.</p> <p>Authorized access will be limited to System and Site users with a need to know.</p>
Monitoring	
<p>17. Will this information system provide the capability to identify, locate, and monitor individuals?</p>	No. The system does not track the physical identity or location of individuals, nor does it monitor their personal behavior. The system contains basic contact information which may potentially be used to help locate individuals. Administrator reviews of audit logs will help prevent any unauthorized monitoring or user behaviors
<p>18. What kinds of information are collected as a function of the monitoring of individuals?</p>	N/A
<p>19. Are controls implemented to prevent unauthorized monitoring of individuals?</p>	N/A



PRIVACY IMPACT ASSESSMENT:
Office of the Chief Information Officer – UnitySync
PIA Template Version 5 – August 2017

MODULE II – PII SYSTEMS & PROJECTS

DATA MANAGEMENT & MAINTENANCE

<p>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.</p>	<p>The data in the system is mostly provided by members of DOE employees and contractors.</p> <p>Within the organization, individual can enter their own information and to ensure that it is current.</p> <p>Therefore, data regarding individuals is generally checked by staff for accuracy, relevancy, and completeness at the time it is received and acknowledged.</p>
<p>21. If the information system is operated in more than one site, how will consistent use of the information be ensured at all sites?</p>	<p>There are three types of Hubs and Spoke configurations.</p> <p>Site A allows the HQ UnitySync (border directory) server to push (write) and pull (read) directly into Site A's live Active Directory (AD).</p> <p>Site B runs their own copy of UnitySync (border directory) and allows HQ UnitySync (border directory) server to push (write) and pull (read) directly into Site B's UnitySync (border directory) server. Site B then manages their own UnitySync (border directory) to pull (read) their contact objects to their UnitySync (border directory), and their UnitySync (border directory) writes directly into their AD.</p> <p>Site C runs their own copy of UnitySync (border directory) and allows HQ UnitySync (border directory) server to ONLY pull (read) contact objects. Site C then manages their own UnitySync (border directory) to pull (read) their contact objects to their UnitySync (border directory), and their UnitySync (border directory) writes directly into their AD. Site C's UnitySync (border directory) also pull (read) directly from HQ's UnitySync (border directory) to populate their border directory.</p> <p>The UnitySync 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 from.</p>
Records Management	
<p>22. Identify the record(s).</p>	<p>No</p> <p>UnitySync does not store or collect</p>



PRIVACY IMPACT ASSESSMENT:
Office of the Chief Information Officer – UnitySync
PIA Template Version 5 – August 2017

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. <input type="checkbox"/> Unscheduled <input type="checkbox"/> Scheduled (<i>cite NARA authority(ies) below</i>) All emails sent by UnitySync are maintained by the DOE e-mail system, all e-mail is maintained for a minimum of 7 years, as stated by the DOE records management office. UnitySync is a Transitory data
24. Records Contact	Virginia Elharam Virginia.elharam@hq.doe.gov 301-903-1468

ACCESS, SAFEGUARDS & SECURITY



PRIVACY IMPACT ASSESSMENT:
 Office of the Chief Information Officer – UnitySync
 PIA Template Version 5 – August 2017

MODULE II – PII SYSTEMS & PROJECTS

<p>25. What controls are in place to protect the data from unauthorized access, modification, or use?</p>	<p>All accounts are “Individual” accounts, and the system contains no other account types (including shared, group, system, guest, emergency, developer, temporary, and service) nor will requests for those account types be approved. In adherence with a “least-privileged access strategy,” security roles are removed from accounts once deemed no longer necessary.</p> <p>To be granted any of the System Roles for the UnitySync application, a user must first meet the following access requirements to be added to any environment:</p> <ul style="list-style-type: none"> • Enabled in Active Directory • Has an active license • Member of the environment’s security group <p>Application system roles, except for the System Administrator, cannot change any security, access, or other configuration settings.</p> <p>Technical and administrative controls are in place to prevent the misuse of data by individuals with access. These access controls are part of the UnitySync System Security Plan (SSP).</p> <p>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.</p> <p>The technical controls include restricted access via unique user-id and password with access/functional privileges to UnitySync.</p> <p>All system team members (federal and contractor) are required to annually complete the Department of Energy Headquarters Annual Cyber Security Refresher Briefing and the Annual Privacy Training as a requirement for access to the system.</p>
<p>26. Who will have access to PII data?</p>	<p>DOE federal and contractor personnel will have access to data in the system including UnitySync System Administrator. Authorized access will be limited to users with a need-to-know basis and separation of duties between system administrators who have limited access to PII and site administrators and users who may upload PII.</p>
<p>27. How is access to PII data determined?</p>	<p>The application System Owner and/or Client Stakeholder determine a Federal or Contractor employee access to the data within the UnitySync application. Once access is approved, the following criteria must be met:</p> <ul style="list-style-type: none"> • Enabled in Active Directory • Has an active license • Member of the environment’s security group



PRIVACY IMPACT ASSESSMENT:
Office of the Chief Information Officer – UnitySync
PIA Template Version 5 – August 2017

MODULE II – PII SYSTEMS & PROJECTS

28. Do other information systems share data or have access to the data in the system? If yes, explain.	UnitySync shares information with DOE Active Directory and other DOE field sites.
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?	Where required, there are Memorandums of Understanding /Agreements (MOUs/MOAs) between DOE EITS and other sites utilizing the UnitySync instance.
30. Who is responsible for ensuring the authorized use of personal information?	DOE Federal Sponsor and UnitySync System Owner, The UnitySync Authorizing Official, as identified in the System Security Plan are responsible for the information contained in their instances of UnitySync.

END OF MODULE II



PRIVACY IMPACT ASSESSMENT:
Office of the Chief Information Officer – UnitySync
PIA Template Version 5 – August 2017

SIGNATURE PAGE		
	Signature	Date
System Owner	<p>Damon Bragg</p> <hr/> <p>(Print Name)</p> <hr/> <p>(Signature)</p>	<hr/>
Local Privacy Act Officer	<hr/> <p>(Print Name)</p> <hr/> <p>(Signature)</p>	<hr/>
Chief Privacy Officer	<p>Ken Hunt</p> <hr/> <p>(Print Name)</p> <hr/> <p>(Signature)</p>	<hr/>