

**EXIM AGILQUEST SYSTEM  
PRIVACY THRESHOLD ANALYSIS (PTA)  
PRIVACY IMPACT ASSESSMENT (PIA)**



**Version 1.1**

**OCTOBER 2022**

**REVISION HISTORY**

<b>VERSION</b>	<b>DATE</b>	<b>AUTHOR</b>	<b>UPDATE SUMMARY</b>
1.0	8/22/2022	Selma Hamilton	Initial document
1.1	10/31/2022	Christina Entzian	POC review and update

**Privacy Threshold Analysis (PTA)**

**SYSTEM INFORMATION**

<b>SYSTEM INFORMATION</b>	
<b>System Name:</b>	AgilQuest Tango Reserve
<b>System Type:</b>	<input checked="" type="checkbox"/> Major Application <input type="checkbox"/> General Support System <input type="checkbox"/> Minor Application
<b>System Categorization (per FIPS 199)</b>	<input type="checkbox"/> High <input type="checkbox"/> Moderate <input checked="" type="checkbox"/> Low
<b>System Description:</b>	<p>Tango Reserve (formerly Forum) is a SaaS platform provided by AgilQuest Corporation, a certified Veteran-Owned Small Business (VOSB). It manages, measures, and schedules meeting rooms, conference rooms, workspaces (permanently assigned, hoteling, and free address) and other workplace resources such as equipment, services, and parking.</p> <p>It provides freedom and flexibility for the workforce while delivering workplace control, actual utilization measurement and decision support for management.</p> <p>Tango Reserve is a FedRAMP compliant cloud-based, SaaS platform that ultimately helps organizations to reduce costs and comply with government mandates including “Reduce the Footprint”, reducing energy costs, improved sustainability, and telework adoption and reporting.</p> <p>With Tango Reserve, EXIM can:</p> <ul style="list-style-type: none"> <li>• Increase workspace flexibility and engage employees;</li> <li>• Improve decision support through workplace utilization data analytics;</li> <li>• Decrease the cost of installations, infrastructure support, and ongoing upgrades;</li> <li>• and Improve office space utilization and ROI through space-sharing opportunities (examples: adding more people within the current workspace footprint, consolidating floors or buildings to leverage excess capacity, sharing excess capacity between organizations).</li> </ul> <p>It supports employee flexibility and makes it easy to find the best place to work, share available assets and optimize the workplace. It can also be used for contact tracing in the event of an outbreak such as COVID-19.</p>
<b>System Owner’s Information (Name, Address, Contact Information)</b>	<p>Courtney Chung                      Senior VP and Chief Management Officer (CMO)                      Export Import Bank of the United States                      811 Vermont Ave. NW, Office 1040   Washington, DC 20571                      (202)-565-3787</p>

**CONTROLLED UNCLASSIFIED INFORMATION (CUI)**

	<a href="mailto:Courtney.Chung@exim.gov">Courtney.Chung@exim.gov</a>
<b>POC Information (Name, Address, Contact Information)</b>	Alan Foust Director of Facility Services and Capital Planning Export Import Bank of the United States 811 Vermont Ave. NW, Office 1040   Washington, DC 20571 202-565-3319 202-578-2372 <a href="mailto:Alan.Foust@exim.gov">Alan.Foust@exim.gov</a>
<b>CISO and CPO Information (Name, Address, Contact Information)</b>	Christopher Sutton III Chief Information Security Officer (CISO) and Chief Privacy Officer (CPO) Export Import Bank of the United States 811 Vermont Ave. NW, Office 1040   Washington, DC 20571 202-336-4388 202-565-3859 <a href="mailto:Christopher.Sutton@exim.gov">Christopher.Sutton@exim.gov</a>

**Questions**

<b>STATUS OF THE INFORMATION SYSTEM:</b>	
2.1	<input checked="" type="checkbox"/> New information system - Implementation date: 9/29/2023 <input type="checkbox"/> Upgraded or Major Modification information system - Upgrade date: Click or tap to enter a date. <input type="checkbox"/> Information system in use without prior authorization <input type="checkbox"/> Information system in use with prior authorization  If this is a new information system, please skip to <b>Question 2.5</b>
2.2	<i>Has this information system existed under another name, or has the name been changed or modified?</i> <input type="checkbox"/> Yes <input type="checkbox"/> No
2.3	<i>Has this information system existed previously or been operated under any other software program, information system medium, i.e., electronic database or paper files, and/or other format?</i> <input type="checkbox"/> Yes <input type="checkbox"/> No
2.4	<i>Has this information system existed under a system of records notice (SORN) by itself, or part of another SORN?</i> <input type="checkbox"/> Yes <input type="checkbox"/> No

**CONTROLLED UNCLASSIFIED INFORMATION (CUI)**

Date Changed	Previous Name/System	Previous SORN #, if applicable

**INFORMATION BEING COLLECTED BY THE SYSTEM:**

2.5 *Does the system collect any Personally Identifiable Information (PII) or/and Business Identifiable Information (BII)?* Yes No  
 If No, please skip to Question 2.7

2.6 *What kind of PII/BII is the system collecting, analyzing, managing, storing, and transferring?*

Personal Information about EXIM Employees  
 Personal Information about EXIM Contractors  
 Information about EXIM Volunteers, Visitors, Customers, and other Individuals  
 Information about Business Customers  
 Non-personal information from businesses and other for-profit entities  
 Non-personal information from institutions and other non-profit entities  
 Non-personal information from Federal Government agencies  
 Non-personal information from state, local governments  
 Others Source, Please Specify:

The system will include the names of EXIM employees and contractors [First Name and Last Name] along with their respective official work email address.

**SYSTEM INTERCONNECTIONS**

2.7 *Is the Information System connected or linked to another system?*  
Yes No  
 If No, please skip to **Question 2.9**

2.8 *If the information system is connected to another system, what PII/BII has been collected by the other system?*

Personal Information about EXIM Employees  
 Personal Information about EXIM Contractors  
 Information about EXIM Volunteers, Visitors, Customers, and other Individuals  
 Information about Business Customers

**CONTROLLED UNCLASSIFIED INFORMATION (CUI)**

- Non-personal information from businesses and other for-profit entities
- Non-personal information from institutions and other non-profit entities
- Non-personal information from Federal Government agencies
- Non-personal information from state, local governments
- Others Source, Please Specify:

Tango Reserve will be linked to EXIM’s MS Exchange system for the purpose of allowing users to book conference rooms and other collaboration spaces. Individual “touchdown” or “hotspot” spaces will not be reservable through the MS Exchange integration – all individual spaces must be booked via the Tango Reserve web or mobile application using the individual user’s login (which is based on the employee’s/CTR’s first name, last name, and government email address – PII).

Systems that Reserve will link to:

1. **Reserve + M365 (Exchange) Integration** – AQ’s Connector to M365 will be registered as an App in EXIM’s Azure.
2. **User Management Process** – The user data will be uploaded either via a server EXIM will host in EXIM’s network, or via EXIM’s AWS account.
3. **Open Presence Listener** – EXIM would send presence events using the Reserve API
4. **SAML** – authentication via EXIM’s IdP

**INFORMATION RETRIEVAL**

2.9 *Is information retrieved from the Information System by a name or a “unique identifier” linked to an individual, e.g., SSN, name, home telephone number, fingerprint, etc.?*

- Yes, then SORN is required
- No

## Analysis

Based on the information that you have provided, if you answered **NO** to **ALL** of questions **2.2**, **2.3**, **2.4**, **2.5**, **2.7**, and **2.9**, then the System does **not** require a Privacy Impact Assessment (PIA).



PIA REQUIRED
NO
<input type="checkbox"/>

If you answered **yes** to **ANY** of the above questions, then the System **requires** a Privacy Impact Assessment (PIA).

PIA REQUIRED
YES
<input checked="" type="checkbox"/>

PRIVACY IMPACT ASSESSMENT (PIA)

A	DATA IN THE SYSTEM
1.	<p><i>Please describe the information to be used in the system. Where possible, be specific, to include any fields entered in tables.</i></p> <div style="border: 1px solid black; padding: 10px;"> <p>The information used in the system to manually create an account from the platform itself is the first and last name of all EXIM employees and EXIM contractors as well as their official EXIM-provided government email address. For the bulk User Management Process (UMP) the REQUIRED fields are:</p> <ul style="list-style-type: none"> <li>• Last Name               <ul style="list-style-type: none"> <li>○ Text Only</li> </ul> </li> <li>• First Name               <ul style="list-style-type: none"> <li>○ Text Only</li> </ul> </li> <li>• Primary Email Address               <ul style="list-style-type: none"> <li>○ Alphanumeric</li> </ul> </li> <li>• Status               <ul style="list-style-type: none"> <li>○ Active or Inactive only</li> </ul> </li> <li>• Language               <ul style="list-style-type: none"> <li>○ English is the most used entry</li> </ul> </li> <li>• Location               <ul style="list-style-type: none"> <li>○ This must match case sensitive to a location in your Reserve</li> </ul> </li> <li>• User Role               <ul style="list-style-type: none"> <li>○ This must be one of the four roles in Reserve: Registered User, Community Manager, Manager or Administrator</li> </ul> </li> <li>• User Group               <ul style="list-style-type: none"> <li>○ This must match case sensitive to an existing User Group in Reserve</li> <li>○ This entry must follow a specific format: {{`User Group Name`}}</li> </ul> </li> <li>• Maximum Days in Advance for Reservations               <ul style="list-style-type: none"> <li>○ Numerical</li> </ul> </li> <li>• Maximum Number of Simultaneous Workspace Reservations               <ul style="list-style-type: none"> <li>○ Numerical</li> </ul> </li> <li>• Bump               <ul style="list-style-type: none"> <li>○ TRUE or FALSE</li> </ul> </li> <li>• Make Assets Available When Bumped               <ul style="list-style-type: none"> <li>○ TRUE or FALSE</li> </ul> </li> <li>• Auto Bump               <ul style="list-style-type: none"> <li>○ TRUE or FALSE</li> </ul> </li> <li>• Make Assets Available When Auto Bumped               <ul style="list-style-type: none"> <li>○ TRUE or FALSE</li> </ul> </li> </ul> </div>



**CONTROLLED UNCLASSIFIED INFORMATION (CUI)**

---

	<p>The system will also allow for additional employee data to be added in future integrations. These “optional fields” must be built into the initial system capabilities by the vendor, but they can be left blank, as place holders, until such time as EXIM decided it is desirable and reasonable to use them. Optional fields will be fields such as “Middle Initial”, “Preferred Name”, “Department”, “Work Phone”, etc.</p> <p>Further/future integrations will also supply employee location metadata to the system for contract tracing and compliance tracking purposes. It is not known at this time what form the metadata will take and a second PIA may be necessary before implementing the OPL integration once more information is available.</p>
2.	<p><i>What are the sources of the information in the system?</i></p> <p>The sources of the information in the system are all data provided from EXIM. User accounts (employee first name, last name, and government email address) can be created individually within the portal or uploaded via a Data Management Utility tool (DMU) bulk uploader application as part of the User Management Process (UMP).</p> <p>The UMP can be performed via EXIM-hosted Server or a serverless UMP.</p> <p>EXIM IT has advised that EXIM will use the EXIM-hosted Server option with Active Directory (AD).</p> <p>EXIM-hosted Server The User Management Process (UMP) allows a client to transform their user HR data extract into the appropriate format required for the AgilQuest Reserve Data Management Utility tool which takes formatted .csv (Comma Separated Value) files as input. The process is implemented through a database driven ETL (Extract, Transform, Load) process which uses tables and functions/stored procedures that can be created using a database platform (RDBMS) of the clients choosing (i.e., MS SQL Server, Oracle, PostgreSQL, MySQL, etc.) The ETL "Extract" is the client source file produced by the client from their HR source system (i.e., AD, Peoplesoft, etc.). The ETL "Load" is handled by the Data Management Utility tool (provided by AgilQuest with associated documentation as needed).</p> <p>Further details about the UMP (such as AWS environment requirements, architecture diagrams, data flow diagrams, etc.) are available by contacting the SO/POC Christina Entzian. &lt;CONT. NEXT PAGE&gt;</p>

**CONTROLLED UNCLASSIFIED INFORMATION (CUI)**

---

	<div style="border: 1px solid black; padding: 10px; margin: 10px auto; width: 80%;"><p>Future integrations to allow for employee location analytics will require data from building turnstiles which is then programmed/formatted by EXIM IT into a compatible data format for the AgilQuest Tango Reserve OPL (Open Presence Listener) integration.</p></div>
a.	<p><b><i>What EXIM Bank files and databases are used?</i></b></p> <div style="border: 1px solid black; padding: 10px; margin: 10px auto; width: 80%;"><p>Active/Staff Directory will be used for the initial source for the database for the system for User creation. The assigned system administrator/Admin User(s) will be responsible for adding and deleting users from the system.</p><p>EXIM will provide a file to the OPL integration at a future date when the data source has been identified, tested/verified, and programmed into an acceptable format.</p></div>
b.	<p><b><i>What Federal Agencies are providing data for use in the system?</i></b></p> <div style="border: 1px solid black; padding: 10px; margin: 10px auto; width: 80%;"><p>EXIM Bank is the only Federal Agency providing data for use in the system. Initial turnstile/badging data is collected from Veterans Affairs (VA) and provided to EXIM. EXIM then formats the data and provides it to the system.</p></div>
c.	<p><b><i>What State and Local Agencies are providing data for use in the system?</i></b></p> <div style="border: 1px solid black; padding: 10px; margin: 10px auto; width: 80%;"><p>None. No State and/or Local Agencies are providing data for use in the system.</p></div>
d.	<p><b><i>What other third-party sources will data be collected from?</i></b></p> <div style="border: 1px solid black; padding: 10px; margin: 10px auto; width: 80%;"><p>None. The system will not collect data from any other third-party sources.</p></div>

**CONTROLLED UNCLASSIFIED INFORMATION (CUI)**

---

e.	<p><i>What information will be collected from clients, customers, or the general public?</i></p> <div style="border: 1px solid black; padding: 10px;"><p>Since the system features a Microsoft Exchange integration for the purpose of reserving meeting and collaboration spaces, and the reservations may include email address information that is not solely limited to EXIM, it is possible that the system could view information such as first name, last name, and email address from parties outside of EXIM from the email itself for the purpose of scheduling those spaces. However, the system does not add users outside of the UMP and/or EXIM Admin User manual account creation. To this end, there is no evidence that the system will “collect” information from clients, customers, or the public.</p></div>
3.	<p><i>How is integrity of the data assured? In other words, how is the data protected from unauthorized changes, modifications, or removal.</i></p> <div style="border: 1px solid black; padding: 10px;"><p>The integrity of the data is assured by setting up User accounts with the correct level of access commensurate with their need to interact with the system. The rule of least privileged access for user accounts will be implemented. Very few accounts will have the access level with permissions to make changes, modifications, or remove data. Additionally, SAML authentication will be used to ensure that User Accounts are only being accessed by the intended user. The UMP, using EXIM-provided AD data, will run nightly to add, modify, and/or delete (make inactive/archive) data, and validate data and is the System of Truth. Data flows through the UMP in one direction, so the EXIM-provided AD data can overwrite the Reserve system data, but the Reserve data does not have reciprocal permissions.</p></div>
a.	<p><i>How will data collected from sources other than EXIM Bank records and the client, customer or public user’s identity be verified for accuracy?</i></p> <div style="border: 1px solid black; padding: 10px;"><p>N/A. All Data collected will come from EXIM Bank records and/or be data uploaded by the individual user such as language preference, account preferences, etc.</p></div>
b.	<p><i>How will data be checked for completeness?</i></p> <div style="border: 1px solid black; padding: 10px;"><p>The data will be checked for completeness by verifying User Accounts against EXIM FTE and CTR employee data (first name, last name, email address) via Active Directory (AD). The UMP will ensure that the complete data required to create and maintain accounts is gathered when the UMP is run.</p></div>

CONTROLLED UNCLASSIFIED INFORMATION (CUI)

c.	<p><i>Is the data current? How do you know?</i></p> <div data-bbox="264 258 1333 909" style="border: 1px solid black; padding: 10px;"><p>The data is received from Active Directory (AD) which is how EXIM IT maintains EXIM employee (FTE and CTR) user accounts. The data in the Reserve system will remain current by running the UMP on a schedule (nightly). There are certain data elements that, as a standard, are updated every time the UMP runs. Things like, first name, last name, email address etc. where the source of truth is EXIM's source system (Active Directory). This means that the information must be correct in EXIM's source system, which will then allow the data to flow into Reserve via the UMP.</p><p>So, the data flow is from EXIM's source system (the "source of truth"). It doesn't flow from Reserve into EXIM's source system. On the other hand, there could be some data elements on the user's profile where EXIM decides (during the requirements gathering) should only be made in Reserve during the initial creation of the user's record and not update every time the UMP runs. This means that a user can modify that field in their profile, and it will not get changed by the UMP (like for Location or Preferred Name).</p></div>
4.	<p><i>Are the data elements described in detail and documented? If yes, what is the name of the document?</i></p> <div data-bbox="264 1062 1333 1161" style="border: 1px solid black; padding: 10px;"><p>Yes. The data elements are described in detail and documented in the "ADD USER Required Fields.pdf".</p></div>

<b>B ACCESS TO THE DATA</b>	
1	<p><i>Who will have access to the data in the system (Users, Managers, System Administrators, Developers, Other)?</i></p> <div data-bbox="264 1365 1333 1541" style="border: 1px solid black; padding: 10px;"><p>Users will only have rights to manage specific parts of their user profile (ex: Preferred Name, Middle Initial, Email Notifications for Reservations) and make reservations for their respective profile. The Administrators will have rights to manage the system and grant privileges to other users/user roles as required.</p></div>
2	<p><i>How is access to the data by a user determined? Are criteria, procedures, controls, and responsibilities regarding access documented?</i></p>

	<p>Access to data will be determined by a need-to-know/rule-of-least-privilege basis. All users will be initially granted the least-privileged user account until and unless it can be determined that they require a higher privileged user account. Standard Operating Procedures are being developed to establish rules for creating User Rolls and User Groups and establishing the process for determining which users require expanded permissions. The documents <a href="#">“Reserve Default User’s Rights by Role – Tango Analytics Support.pdf”</a> and <a href="#">“Reserve User Roles – Tango Analytics Support.pdf”</a> are provided as artifacts and will be used as “Best Practices” to inform our SOP for user rights, rolls, and permissions.</p>
3	<p><i>Will users have access to all data on the system or will the user’s access be restricted? Explain.</i></p> <p>Access to data will be determined by a need-to-know/ rule-of-least-privilege basis. All users will be initially granted the least-privileged user account until and unless it can be determined that they require a higher privileged user account. Standard Operating Procedures are being developed to establish rules for creating User Rolls and User Groups and establishing the process for determining which users require expanded permissions. The documents <a href="#">“Reserve Default User’s Rights by Role – Tango Analytics Support.pdf”</a> and <a href="#">“Reserve User Roles – Tango Analytics Support.pdf”</a> are provided as artifacts and will be used as “Best Practices” to inform our SOP for user rights, rolls, and permissions.</p>
4	<p><i>What controls are in place to prevent the misuse (e.g., browsing) of data by those having legitimate access?</i></p>

**CONTROLLED UNCLASSIFIED INFORMATION (CUI)**

	<p>Access to data will be determined by a need-to-know/rule-of-least-privilege basis. All users will be initially granted the least-privileged user account until and unless it can be determined that they require a higher privileged user account. Standard Operating Procedures are being developed to establish rules for creating User Rolls and User Groups and establishing the process for determining which users require expanded permissions. The documents “<a href="#">Reserve Default User’s Rights by Role – Tango Analytics Support.pdf</a>” and “<a href="#">Reserve User Roles – Tango Analytics Support.pdf</a>” are provided as artifacts and will be used as “Best Practices” to inform our SOP for user rights, rolls, and permissions.</p> <p>Additionally, since the data being collected by the system is largely data that can already be accessed by EXIM employees (for example, searching EXIM’s Microsoft Outlook with show employee first name, last name, email address, plus more data such as phone number (office and mobile) and office location) there would be no tangible benefit to an Admin User looking at the user data in Reserve.</p>
5	<p><b><i>Does the program or application collect, or store information related to a customer or employee where data is retrieved by name, unique number, symbol, or another identifier assigned to the customer or employee?</i></b></p> <p>Yes <input checked="" type="checkbox"/> No <input type="checkbox"/></p>
a.	<p><b><i>Do other systems share data or have access to data in this system?</i></b></p> <p>Yes <input checked="" type="checkbox"/> No <input type="checkbox"/> If yes, explain.</p> <div data-bbox="272 1283 1344 1423" style="border: 1px solid black; padding: 5px;"> <p>EXIM’s server will share data to the Reserve system via the UMP. EXIM’s Microsoft (M365) Exchange will integrate with the Reserve system to allow for the reservation of meeting rooms and collaboration spaces in either system.</p> </div>
b.	<p><b><i>Who will be responsible for protecting the privacy rights of the external users (customers) affected by the system?</i></b></p> <div data-bbox="261 1539 1333 1598" style="border: 1px solid black; padding: 5px;"> <p>External users will not be added to or affected by the system.</p> </div>
6.	<p><b><i>Who else will have access to the data?</i></b></p>

**CONTROLLED UNCLASSIFIED INFORMATION (CUI)**

	<p>Once the data lives in the Reserve system, only privileged user accounts will have access to the data. Privileged user accounts will include EXIM Admin Users as well as the possibility of AQ Admin Users. AQ can leave their Admin account in there or remove it after the implementation period, at EXIM's request. Most AQ customers choose to leave the AQ Admin account active for support purposes, however it is not a requirement.</p>
a.	<p><i>Will other agencies share data or have access to data in this system (International, Federal, State, Local, Other)?</i></p> <p>Yes <input type="checkbox"/> No <input checked="" type="checkbox"/></p>
b.	<p><i>How will the data be used by the agency?</i></p> <p>The data in the system will be used to show:</p> <ul style="list-style-type: none"> <li>• the total number of EXIM personnel that will be in the facility on a given day</li> <li>• who is in the facility</li> <li>• their location</li> <li>• forecasting for employee location in the future (location added by the employee per supervisor direction)</li> <li>• the location of IT assets within spaces</li> <li>• as an IT Asset Location Log</li> <li>• to understand facility usage for capital planning and space utilization/maximization</li> <li>• to allow for contact tracing</li> <li>• to perform analytics for EXIM decision-makers use in confirming employee compliance to regulations</li> <li>• although it is not EXIM's system for emergencies it may provide benefits in an emergency</li> <li>• it MAY also allow for EXIM personnel to reserve parking in the facility on a day that they will be in the office</li> </ul>

<b>C ATTRIBUTES OF THE DATA</b>	
1.	<p><i>Is the use of the data both relevant and necessary to the purpose for which the system is being designed?</i></p> <p>Yes <input checked="" type="checkbox"/> No <input type="checkbox"/></p>

**CONTROLLED UNCLASSIFIED INFORMATION (CUI)**

2.	<p><i>What personal information and/or personally identifiable information does the system contain?</i></p> <div style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <p>First/Last Name, email address (REQUIRED)                  Middle Initial, Preferred Name (OPTIONAL)                  Location/office, forecasted schedule (AFTER RESERVATION IS MADE)</p> </div>
a.	<p><i>Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected?</i></p> <p>Yes <input checked="" type="checkbox"/> No <input type="checkbox"/></p>
b.	<p><i>Will the new data listed in (a.) above be placed in the individual's record (client, customer, or public user)?</i></p> <p>Yes <input checked="" type="checkbox"/> No <input type="checkbox"/></p>
c.	<p><i>Can the system make determinations about clients, customers or public users that would not be possible without the new data?</i></p> <p>Yes <input checked="" type="checkbox"/> No <input type="checkbox"/></p>
d.	<p><i>How will the new data be verified for relevance and accuracy?</i></p> <div style="border: 1px solid black; padding: 10px; margin: 10px 0;"> <p>The new data will be employee location data that shows what workspaces a user has booked in the system and what spaces they plan to use in the future (if forecasting is implemented) (INITIAL). Accuracy will be determined by spot checks of who is sitting where in the facility. Relevance of the data will be determined by Facilities to see which analytics support the objective of capital planning and space management. Future data, after badging information is acquired by EXIM and loaded into the system, will be to allow for data analytics of the badging (employee location data). That data will be verified for accuracy by comparing it to the EXIM source file. All badging data will be relevant.</p> </div>
3.	<p><i>What controls are in place to protect information during consolidation?</i></p> <div style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <p>The data is processed in-system, which FedRAMP Authorized. During consolidation the information will have the same level of protection as all the other data in the system.</p> </div>
a.	<p><i>If data is being consolidated, what controls are in place to protect the data from unauthorized access or use?</i></p>



CONTROLLED UNCLASSIFIED INFORMATION (CUI)

	<p>The controls in place to protect the data from unauthorized use are:</p> <ul style="list-style-type: none"><li>• setting up User accounts with the correct level of access commensurate with their need to interact with the system</li><li>• the rule of least privileged access for user accounts.</li><li>• very few accounts will have the permissions to access or use the data</li><li>• SAML authentication will be used to ensure that User Accounts are only being accessed by the intended user</li></ul>
b.	<p><i>If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? Explain.</i></p> <p>The proper controls will be in place to protect the data and prevent unauthorized access by setting up User accounts with the correct level of access commensurate with their need to interact with the system. The rule of least privileged access for user accounts will be implemented. Very few accounts will have the access level with permissions to make changes, modifications, or remove data. Additionally, SAML authentication will be used to ensure that User Accounts are only being accessed by the intended user. The UMP, using EXIM-provided AD data, will run nightly to add, modify, and/or delete (make inactive/archive) data, and validate data and is the System of Truth. Data flows through the UMP in one direction, so the EXIM-provided AD data can overwrite the Reserve system data, but the Reserve data does not have reciprocal permissions.</p>
4.	<p><i>How will the data be retrieved? Can data be retrieved by personal identifier?</i></p> <p>Yes <input checked="" type="checkbox"/> No <input type="checkbox"/></p> <p>If yes, explain.</p> <p>Data will be retrieved by Admin users/Privileged users logging into the system. From the system, reports and analytics can then be run (data retrieved). Reports can be run using a personal identifier (example: locations for which a specific user had made a reservation for a period). The reports can be printed in PDF format for presentation to senior leadership and/or EXIM decision-makers.</p>
5.	<p><i>What are the potential effects on the due process rights of clients, customers, or public users...?</i></p> <p>None. The system will not affect EXIM clients, customers, or public users.</p>

**CONTROLLED UNCLASSIFIED INFORMATION (CUI)**

a.	<p><i>...consolidation and linkage of files and systems;</i></p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;">None. The system will not affect EXIM clients, customers, or public users.</div>
b.	<p><i>...derivation of data; accelerated information processing and decision making; and</i></p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;">None. The system will not affect EXIM clients, customers, or public users.</div>
c.	<p><i>...use of new technologies.</i></p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;">None. The system will not affect EXIM clients, customers, or public users.</div>

<b>D</b>	<b>MAINTENANCE OF ADMINISTRATIVE CONTROLS</b>
1.	<p><i>Does the system ensure equitable treatment of individuals or groups of people?</i></p> <p>Yes <input checked="" type="checkbox"/> No <input type="checkbox"/></p>
a.	<p><i>Explain how the system and its use will ensure equitable treatment of clients, customers or general public users.</i></p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;">The system ensures equitable treatment of EXIM FTEs and CTRs by assigning permissions via User Role, which is determined by the Rule of Least Privilege, Need-to-know, and job function. (Example: Facilities, HR, etc.) The system will not be accessed or available to EXIM clients, customers, or public users.</div>
b.	<p><i>If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?</i></p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;">The system is operated on AgilQuest's FedRAMP Authorized AWS Server only.</div>
c.	<p><i>Explain any possibility of disparate treatment of individuals or groups.</i></p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;">There are no foreseeable possibilities of disparate treatment of individuals or groups.</div>

**CONTROLLED UNCLASSIFIED INFORMATION (CUI)**

2.	<p><i>What are the procedures for archiving and retaining information in the system?</i></p> <div style="border: 1px solid black; padding: 5px;"> <p>Information in the system is “archived” rather than deleted. The procedures for archiving data will be the nightly running of the UMP which updates all user accounts, including the archiving and/or making “inactive” user accounts. The UMP uses EXIM’s AD to maintain the most recent version of user accounts and acts as the “Source of Truth” for the system.</p> </div>
a.	<p><i>What are the retention periods of data in this system?</i></p> <div style="border: 1px solid black; padding: 5px;"> <p>Data in the system is “archived” rather than deleted. The data will be retained if EXIM continues to procure the licenses to the AQ Reserve system. Data maintenance is covered in AQ’s FedRAMP package. If EXIM terminates, AQ shuts down the instance of Reserve. EXIM can advise AQ of how long to keep a backup. Once the instance is cancelled however all the data is anonymized.</p> </div>
b.	<p><i>What are the procedures for eliminating the data at the end of the retention period? Where are the procedures documented?</i></p> <div style="border: 1px solid black; padding: 5px;"> <p>Data maintenance is covered in AQ’s FedRAMP package. If EXIM terminates, AQ shuts down the instance of Reserve. EXIM can advise AQ of how long to keep a backup. Once the instance is cancelled however all the data is anonymized.</p> </div>
c.	<p><i>While the data is retained in the system, what are the requirements for determining if the data is still sufficiently accurate, relevant, timely, and complete to ensure fairness in making determinations?</i></p> <div style="border: 1px solid black; padding: 5px;"> <p>The requirements are that the data is verified, updated, and maintained by the nightly UMP process from EXIM’s source of truth data (EXIM’s AD).</p> </div>
3.	<p><i>Does the system use new technology and what are the impacts of this technology on privacy?</i></p> <p>Yes <input checked="" type="checkbox"/> No <input type="checkbox"/></p>
a.	<p><i>Is the system using technologies in ways that the EXIM BANK has not previously employed (e.g., Caller-ID)?</i></p> <p>Yes <input checked="" type="checkbox"/> No <input type="checkbox"/></p>

CONTROLLED UNCLASSIFIED INFORMATION (CUI)

b.	<p><i>How does the use of this technology affect clients, customers or general public users' privacy?</i></p> <div data-bbox="264 300 1333 520" style="border: 1px solid black; padding: 5px;"><p>The use of this technology has the potential to impact EXIM bank FTEs and CTRs privacy by allowing privileged users and other users to see location data for that employee. It does not affect EXIM clients, customers, or general public users.</p></div>
4.	<p><i>Does the system provide the capability to track and monitor individuals or groups?</i></p> <p>Yes <input checked="" type="checkbox"/> No <input type="checkbox"/></p>
a.	<p><i>Will this system provide the capability to identify, locate, and monitor individuals?</i></p> <p>Yes <input checked="" type="checkbox"/> No <input type="checkbox"/></p> <p>If yes, explain.</p> <div data-bbox="264 909 1333 1287" style="border: 1px solid black; padding: 5px;"><p>The system is a Hybrid Workspace Management System (HRMS). It exists to allow Users to remotely reserve a workspace for planned time in the office and have access to the right kind of space and IT peripherals to successfully complete their on-office tasks. It also allows other Users to see where an individual will be working that day to enhance workplace collaboration. It also has the potential to serve as a “furcating tool” to see whether or not staff plan to be in the office in the coming weeks. Analytics can then be run to determine space utilizations and reservations by user. The ability to identify, locate, and monitor individuals is a core function of this system.</p></div>
b.	<p><i>Will this system provide the capability to identify, locate, and monitor groups of people? If yes, explain.</i></p> <p>Yes <input checked="" type="checkbox"/> No <input type="checkbox"/></p>
c.	<p><i>What controls will be used to prevent unauthorized monitoring?</i></p> <div data-bbox="264 1583 1333 1730" style="border: 1px solid black; padding: 5px;"><p>Analytics can be run to identify, locate, and monitor User Groups; those User Groups could be formed around certain groups of people (such as CFO staff, HR staff, etc.).</p></div>

**CONTROLLED UNCLASSIFIED INFORMATION (CUI)**

---

5.	<p><i>How will the information in the system be secured?</i></p> <div data-bbox="261 262 1333 363" style="border: 1px solid black; padding: 5px;"><p>The information in the system is secured because it is a FedRAMP Authorized AWS hosted system.</p></div>
a.	<p><i>What are the security controls (administrative, technical, and operational) controls designed to secure the system?</i></p> <div data-bbox="261 514 1333 653" style="border: 1px solid black; padding: 5px;"><p>The security controls are administrative (policy), technical (SAML Authentication), and operational (User Roles of rules of least privilege and Need-to-Know).</p></div>
b.	<p><i>Is the system designating a 'system of records' under the Privacy Act, 5 U.S.C. 552a?</i></p> <p>Yes <input checked="" type="checkbox"/> No <input type="checkbox"/></p>