U.S. Department of Commerce
International Trade Administration (ITA)

Privacy Threshold Analysis
for the
Lotus Notes

U.S. Department of Commerce Privacy Threshold Analysis

ITA/Lotus Notes

Unique Project Identifier: 2384

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system and its purpose: *Provide a general description (in a way that a non-technical person can understand) of the information system that addresses the following elements:*

The E-Government Act of 2002 defines "information system" by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: "Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

a) *Whether it is a general support system, major application, or other type of system*
   Major Application

b) *System location*

   The system is located in AWS on ITA network (DMZ/internal).

c) *Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)*
   Standalone system

d) *The purpose that the system is designed to serve*
   Lotus Notes is an ITA enterprise wide system supporting program units within the ITA, primarily the Global Markets (Commercial Service). The system provides the capability to find the products/services GM posts/offices offer, track client participation in events & services, collect any fee (through Pay.gov), and monitor post/office financial transactions. The Whitepages module is a repository of GM/OCIO employees contact information and employee's emergency contact information (name/phone only). Whitepages is also used to on-board/off-board GM/OCIO employees.

e) *The way the system operates to achieve the purpose*
   The ITA Lotus Notes System is based upon n-tier architecture for flexibility and

reusability. Several servers are being used to support various layers of the system that include web (presentation), application, and database layer. The following section provides a brief description of each layer.

1) Presentation Layer: The topmost layer of the application that displays information related to the services provided by the information system. It communicates with the application layer and sends or displays information via web page (comprising static and dynamic content) to both authenticated and non-authenticated ITA end-users and external clients. The web servers used are IBM HTTP Server (Apache) and IBM Domino HTTP Server running on Windows 2016 platform.

2) Application Layer: Controls application's functionality. It utilizes authentication and authorization services from the infrastructure and communicates with the database and presentation layers. The application servers used are WebSphere Application Server (WAS) and IBM Domino Server running on Windows 2016 platform.

3) Database Layer: Provides data persistence and access layer. The back-end database DB2.

f) *A general description of the type of information collected, maintained, used, or disseminated by the system*
Lotus Notes system captures and disseminates the following: Name, Telephone, Email address, Work email address, Job title, Work address, Work telephone number, User ID, Date/Time of access, and Queries run.

g) *Identify individuals who have access to information on the system*
The Lotus Notes application provides access through a web page/browser and has a distinct user base: End-Users (public users), Local Users and Local Administrators. The end-users have access to the public domain only. The local users and the local administrators have access to the application domain. Local administrators also have administrative access at the system level (i.e., Windows 2016). The rights, privileges, and accesses are different between distinct user groups. The end-users do not have access to the Windows domain and cannot use domain resources. Access is restricted through least privilege principles using the ACL and group roles Therefore, end-users are restricted from performing the functions of local user and/or a local Administrator.

h) *How information in the system is retrieved by the user*
The Lotus Notes application provides access through a web page/browser. Access to Lotus Notes is available from the ITA network. Users must first connect/authenticate to Citrix or Cisco Any Connect prior to gaining access to Lotus Notes. At which point a user must authenticate into Lotus Notes using their Lotus Notes credentials.

i) *How information is transmitted to and from the system*
Information is transmitted through secure HTTPS connections.

Questionnaire:

1. What is the status of this information system?

_____ This is a new information system. *Continue to answer questions and complete certification.*

_____ This is an existing information system with changes that create new privacy risks.
Complete chart below, continue to answer questions, and complete certification.

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					

_X__ This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment. *Continue to answer questions and complete certification.*

_____ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2015). *Continue to answer questions and complete certification.*

_____ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2017 or later). *Skip questions and complete certification.*

1b. Has an IT Compliance in Acquisitions Checklist been completed with the appropriate signatures?

_____ Yes. This is a new information system.

_____ Yes. This is an existing information system for which an amended contract is needed.

_____ No. The IT Compliance in Acquisitions Checklist is not required for the acquisition of equipment for specialized Research and Development or scientific purposes that are not a National Security System.

__X__ No. This is not a new information system.

2. Is the IT system or its information used to support any activity which may raise privacy concerns?
NIST Special Publication 800-53 Revision 4, Appendix J, states "Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary." Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

____   Yes. *(Check all that apply.)*

Activities			
Audio recordings		Building entry readers	
Video surveillance		Electronic purchase transactions	
Other (specify):			

_X___ No.

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

    As per DOC Privacy Policy: "For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)."

    __ _   Yes, the IT system collects, maintains, or disseminates BII.

    __X__ No, this IT system does not collect any BII.

4. Personally Identifiable Information (PII)
4a. Does the IT system collect, maintain, or disseminate PII?

    As per OMB 17-12: "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."

    __X_   Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

    _X__   DOC employees
    ____   National Institute of Standards and Technology Associates
    _X__   Contractors working on behalf of DOC
    ____   Other Federal Government personnel
    ____   Members of the public

    ____   No, this IT system does not collect any PII.

If the answer is "yes" to question 4a, please respond to the following questions.

4

4b. Does the IT system collect, maintain, or disseminate Social Security numbers (SSNs), including truncated form?

    __ _   Yes, the IT system collects, maintains, or disseminates SSNs, including truncated form.

Provide an explanation for the business need requiring the collection of SSNs, including truncated form.
Provide the legal authority which permits the collection of SSNs, including truncated form.

    __X__ No, the IT system does not collect, maintain, or disseminate SSNs, including truncated form.

4c. Does the IT system collect, maintain, or disseminate PII other than user ID?

   _X___ Yes, the IT system collects, maintains, or disseminates PII other than user ID.

   ___   No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4d. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

   ____   Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

   __X_ No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, 4c, and/or 4d are "Yes," a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the approved PIA must be a part of the IT system's Assessment and Authorization Package.

CERTIFICATION

__X__ I certify the criteria implied by one or more of the questions above **apply** to the ITA Lotus Notes and as a consequence of this applicability, I will perform and document a PIA for this IT system.

_____ I certify the criteria implied by the questions above **do not apply** to the ITA Lotus Notes and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of System Owner (SO): __Michael Hunt_____

Signature of SO: Michael Hunt Digitally signed by Michael Hunt Date: 2021.02.12 10:27:35 -05'00'   Date: _____

Name of Information Technology Security Officer (ITSO): __Joe Ramsey_____

Signature of ITSO: Joe Ramsey Digitally signed by Joe Ramsey Date: 2021.02.18 16:56:30 -05'00'   Date: _____

Name of Privacy Act Officer (PAO): __Chad Root (Acting)_____

Signature of PAO: TIMOTHY ROOT Digitally signed by TIMOTHY ROOT Date: 2021.02.09 11:49:06 -05'00'   Date: _____

Name of Authorizing Official (AO): __Rona Bunn_____

Signature of AO: RONA BUNN Digitally signed by RONA BUNN Date: 2021.02.18 17:15:07 -05'00'   Date: _____

Name of Bureau Chief Privacy Officer (BCPO): __Chad Root (Acting)_____

Signature of BCPO: TIMOTHY ROOT Digitally signed by TIMOTHY ROOT Date: 2021.02.09 11:49:27 -05'00'   Date: _____