Version Number: 01-2017

U.S. Department of Commerce
U.S. Patent and Trademark Office

Privacy Threshold Analysis
for the
Consolidated Financial System (CFS)

U.S. Department of Commerce Privacy Threshold Analysis

USPTO Consolidated Financial System

Unique Project Identifier: PTOC-001-00

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 of the information system in a way that a non-technical person can understand.*

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).

Momentum

Momentum is a full-featured Commercial off-the-shelf (COTS) accounting software package that permits full integration of the processing of financial transactions with other normal business processes. The system empowers the USPTO program offices to tie together many financial accounting functions, including plans, purchasing transactions, fixed assets, travel accounting, accounts receivable, accounts payable, reporting, security and workflow processes, general ledger, external reports, budget, payroll and automated disbursements through an integrated relational database.

Concur Government Edition (CGE)

CGE is a web-based travel and planning management solution owned, hosted, maintained and operated by Concur, Inc. In order to support the Federal Government's more broadly defined eTravel 2 (ETS2) program, including funds control, accounting and fiscal management of Agency travel, the USPTO was required to construct an interface between the CGE and Momentum. The CGE application falls within the security boundary of the General Services Administration (GSA) and is authorized to operate by GSA. The USPTO has a Memorandum of Understanding (MOU) and an Interconnection Security Agreement (ISA) in place with GSA for this integration.

eAcquisition Tool (ACQ)

ACQ is a web-based COTS solution to support users in the acquisition community at the USPTO. ACQ allows procurement users to create acquisition plans and track the life of procurement actions and documents associating with the plan. ACQ integrates with Momentum,

Vendor Portal, Enterprise Data Warehouse (EDW), and the Electronic Library for Financial Management Systems (EL4FMS).

VendorPortal
VendorPortal is a web-based COTS solution to provide a platform for interaction and information exchange between USPTO and the vendor community. VendorPortal provides the ability to publish notices, solicitations and award announcements; enables vendor offer, invoice and receipt submission, and provides vendors insight into awards, deliverables and invoice statuses.

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):					

____ 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.*
_X_ 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 or later). *Skip questions and complete certification.*

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. *Please describe the activities which may raise privacy concerns.*

_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.)."

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

_X_ Companies
_X_ Other business entities

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

4. Personally Identifiable Information

4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?

As per OMB 07-16, Footnote 1: "The term 'personally identifiable information' refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc… alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc…"

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

_X_ DOC employees
_X_ Contractors working on behalf of DOC
_X_ 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.

4b. 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.

4c. 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.

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

____ 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, and/or 4c 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 Consolidated Financial System 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 Consolidated Financial System and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of System Owner (SO): Gita Zoks

Signature of SO: Users, Zoks, Gita Digitally signed by Users, Zoks, Gita Date: 2019.03.11 07:56:22 -04'00' Date: _____

Name of Senior Information Security Officer (SISO): John Pardun

Signature of SISO: _____ Date: 3-13-2019

Name of Co-Authorizing Official (Co-AO): Anthony Scardino

Signature of Co-AO: _____ Date: 3/20/19

Name of Authorizing Official (AO) & Bureau Chief Privacy Officer (BCPO): Henry J. Holcombe

Signature of AO & BCPO: _____ Date: 15 MAR 19