Version Number: 01-2015

U.S. Department of Commerce
Office of Inspector General (OIG)

Privacy Threshold Analysis
For the
OIG General Support System (GSS)

U.S. Department of Commerce Privacy Threshold Analysis

OIG/OIG GSS

Unique Project Identifier: IT Infrastructure System (OIG0001)

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:
The OIG General Support System (GSS) provides general operational IT services and support for the mission and activities of the OIG; network user authentication and access; e-mail service; file processing, sharing, and storage; application and database development, update, and management; print services; and overall system security (including patch and antivirus management). The OIG GSS supports all business essential and office automation applications for all OIG components

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. *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.*

____ 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 about: *(Check all that apply.)*

____☐ Companies
____☐ 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..."

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

____☐ DOC employees

____☐ Contractors working on behalf of DOC
____☐ 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?

____ 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.

____ 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

___☐ I certify the criteria implied by one or more of the questions above **apply** to the OIG GSS and as a consequence of this applicability, I will perform and document a PIA for this IT system.

__X__☐ I certify the criteria implied by the questions above **do not apply** to the [IT SYSTEM NAME] and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of Information System Security Officer (ISSO) or System Owner (SO): Stephen Jones

Signature of ISSO or SO: _____ Date: 8/21/17

Name of Information Technology Security Officer (ITSO): TOAN-PHAM

Signature of ITSO: _____ Date: 8/21/2017

Name of Authorizing Official (AO): Robin Berg

Signature of AO: _____ Date: 8/21/17

Name of Bureau Chief Privacy Officer (BCPO): Toan Pham

Signature of BCPO: STEPHEN JONES Digitally signed by STEPHEN JONES DN: c=US, o=U.S. Government, ou=Department of Commerce, ou=Office of the Inspector General, cn=STEPHEN JONES, 0.9.2342.19200300.100.1.1=13001003228551 Date: 2017.09.18 11:04:53 -04'00' Date: 09/18/2017

For Toan Pham