U.S. Department of Commerce Privacy Threshold Analysis
NIST/CBS/CFS

Unique Project Identifier: 162-01

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).

a) Whether it is a general support system, major application, or other type of system
   The NIST Commerce Business System, Core Financial System (CBS/CFS) is a major application.

b) System location
   The system is located at the NIST Gaithersburg, Maryland facility within the continental United States.

c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)
   The NIST Commerce Business System, Core Financial System (CBS/CFS) is a standalone system.

Data is shared with other DOC agencies who utilize NIST financial management and accounting functionality, as well as the DOC Office of Inspector General for purposes of fraud analysis. Data is also shared as follows:
1. E-Gov Travel Service 2 (ETS2) Travel and Authorization Voucher System (TAVS) for employees and associates, and related relocation activities with moveLINQs (mLINQS).
2. General Service Administration System of Award Management (SAM) for vendor information;
3. Department of Agriculture National Finance Center (NFC) for employee payroll expense information;
4. Department of Treasury Automated Standard Application for Payments (ASAP) system for grants payment information;
5. Department of Treasury Bureau of Fiscal Services Payment Automation Manager (PAM) for payments to vendors and employees; and
6. Vendor information to Federal Reserve Bank for use with the Department of Treasury Do Not Pay application.

Data is shared with other Government entities on a case-by-case basis for purposes of fraud, audit, or law enforcement.

d) The purpose that the system is designed to serve
The Commerce Business System, Core Financial System (CBS/CFS) is a tool used by the NIST Chief Financial Officer (CFO) for planning, directing, and implementing the financial management, administrative, facilities and safety programs of NIST and several other Commerce bureaus.

e) The way the system operates to achieve the purpose
The following are examples of transactions using CBS/CFS which may contain Personally Identifiable Information (PII) or Business Identifiable Information (BII):

1. Creating obligation and invoice/payment information based on E-Gov Travel Service 2 (ETS2) Travel and Authorization Voucher System (TAVS), and relocation activities with moveLINQs (mLINQS).
2. Creating invoice/payment information using data from the General Service Administration System of Award Management (SAM) for exchange of goods and services.
3. Using Department of Treasury Automated Standard Application for Payments (ASAP) system to record grantees and release of funds to grantees.
4. Creating an invoice/payment information with Department of Treasury Bureau of Fiscal Services Payment Automation Manager (PAM) for payments to vendors and employees.

f) A general description of the type of information collected, maintained, use, or disseminated by the system
The system contains identifying numbers, general personal data, and work-related data to support financial transactions (e.g. obligation of funds, payments, and refunds for contracts, bankcard purchase, employee travel, property, etc.).

g) Identify individuals who have access to information on the system
NIST internal and other agency authorized users access the CBS/CFS application.

h) How information in the system is retrieved by the user
NIST internal and other agency authorized users access the CBS/CFS application from their desktop through a secure web portal.
i) How information is transmitted to and from the system

Information is transmitted between the components using the Transport layer Security (TLS) protocol, which encrypts communications, or FIPS 140-2 encrypted virtual private network technologies between organizations.

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.

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

____ 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 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.

____ 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 (entities that obtain NIST-issued grants)

____ 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

__X__ I certify the criteria implied by one or more of the questions above apply to the CBS/CFS (162-01) 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 CBS/CFS (162-01) and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of System Owner (SO):
John Quick
Signature of SO: JOHN QUICK Digitally signed by JOHN QUICK
Date: 2019.09.17 11:46:32 -04'00'

Name of Information Technology Security Officer (ITSO):
K. Robert Glenn
Signature of ITSO: KENNETH GLENN Digitally signed by KENNETH GLENN
Date: 2019.09.17 16:22:04 -04'00'

Name of Co-Authorizing Official (AO):
George Jenkins
Signature of Co-AO: ___________
Date: 9/16/17

Name of Co-Authorizing Official (AO)/Bureau Chief Privacy Officer (BCPO):
Susannah Schiller, Acting
Signature of Co-AO/BCPO: SUSANNAH SCHILLER Digitally signed by SUSANNAH SCHILLER
Date: 2019.09.17 16:26:34 -04'00'

Date: ___________