Template Version Number: 01-2021

U.S. Department of Commerce
National Institute of Standards and Technology (NIST)

Privacy Threshold Analysis
for the
162-01 Commerce Business System, Core Financial System (CBS/CFS)

U.S. Department of Commerce Privacy Threshold Analysis

National Institute of Standards and Technology (NIST)

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 brief description of the information system.*

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
b) System location
c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)
d) The purpose that the system is designed to serve
e) The way the system operates to achieve the purpose
f) A general description of the type of information collected, maintained, use, or disseminated by the system
g) Identify individuals who have access to information on the system
h) How information in the system is retrieved by the user
i) How information is transmitted to and from the system

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; Department of Treasury Bureau of Fiscal Services**
5. **Payment Automation Manager (PAM) for payments to vendors and employees.**
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 use the Transport layer Security (TLS) protocol which encrypts communications, or FIPS 140-2 encrypted virtual private network technologies between organizations.

Questionnaire:

1. Status of the Information System

1a. What is the status of this information system?

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.)

Changes That Create New Privacy Risks (CTCNPR)
Other changes that create new privacy risks:

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

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.

Activities
Other activities which may raise privacy concerns:

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.)."

4. Personally Identifiable Information (PII)

4a. Does the IT system collect, maintain, or disseminate sensitive personally identifiable information (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."

The IT system collects, maintains, or disseminates sensitive PII about:

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

4b. Does the IT system collect, maintain, or disseminate Social Security numbers (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.

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

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.

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 SAOP approved PIA must be a part of the IT system's Assessment and Authorization Package.

Is a PIA Required?	**Yes**

CERTIFICATION

_X_ The criteria implied by one or more of the questions above **apply** to the 162-01 Commerce Business System, Core Financial System (CBS/CFS) and as a consequence of this applicability, a PIA will be performed and documented for this IT system.

The criteria implied by the questions above **do not apply** to the 162-01 Commerce Business System, Core Financial System (CBS/CFS) and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Information System Security Officer or System Owner Name: Quick, John Office: 101/A0821 Phone: 301-975-2261 Email: john.quick@nist.gov JOHN QUICK Digitally signed by JOHN QUICK Date: 2022.05.05 08:55:19 -04'00' Signature: ______________ Date signed: ______________	**Chief Information Security Officer** Name: Heiserman, Blair Office: 225/A155 Phone: 301-975-3667 Email: nist-itso@nist.gov Digitally signed by BLAIR HEISERMAN Date: 2022.05.02 16:53:57 -04'00' Signature: ______________ Date signed: ______________
Co-Authorizing Official Name: Jenkins, George Office: 101/A0702 Phone: 301-975-5080 Email: George.jenkins@nist.gov GEORGE JENKINS Digitally signed by GEORGE JENKINS Date: 2022.05.03 07:49:37 -04'00' Signature: ______________ Date signed: ______________	**Authorizing Official** Name: Sastry, Chandan Office: 225/B222 Phone: 301-975-6500 Email: chandan.sastry@nist.gov CHANDAN SASTRY Digitally signed by CHANDAN SASTRY Date: 2022.05.02 16:10:25 -04'00' Signature: ______________ Date signed: ______________
Privacy Act Officer Name: Fletcher, Catherine Office: 101/A523 Phone: 301-975-4054 Email: catherine.fletcher@nist.gov CATHERINE FLETCHER Digitally signed by CATHERINE FLETCHER Date: 2022.05.03 12:59:51 -04'00' Signature: ______________ Date signed: ______________	**Chief Privacy Officer** Name: Barrett, Claire Office: 225/B226 Phone: 301-975-2852 Email: claire.barrett@nist.gov CLAIRE BARRETT Digitally signed by CLAIRE BARRETT Date: 2022.04.29 12:27:53 -04'00' Signature: ______________ Date signed: ______________