Version Number: 01-2017

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

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

Reviewed by: Susannah Schiller, Acting, Bureau Chief Privacy Officer

☒ Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

☐ Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

09/30/2019

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer Date

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

Unique Project Identifier: 162-01

Introduction: System Description

Provide a description of the system that addresses the following elements:
The response must be written in plain language and be as comprehensive as necessary to describe the system

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.

The system provides financial management and accounting functionality, and consists of the following modules:

- Commerce Business System Portal (CP),
- Commerce Purchase Card System (CPCS), and
- Data Warehouse (DW).

These modules provide authorized users with the following functionalities:

- Accounts Payable (Payment Management),
- Accounts Receivable (Receipt Management),
- General Ledger (GL),
- Budget Execution (BOPs),
- Cost Allocation, Reimbursable (Cost Management), and
- Reporting and Workflow Management.

(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. See item (g).

(d) The way the system operates to achieve the purpose(s) identified in Section 4

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.

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.

(e) 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.

(f) 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.

(g) Any information sharing conducted by the 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.

(h) The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information

The National Institute of Standards and Technology Act, as amended, 15 U.S.C. 271 et seq. (which includes Title 15 U.S.C. 272) and section 12 of the Stevenson-Wydler Technology Innovation Act of 1980, as amended, 15 U.S.C. 3710a.;

5 U.S.C. 5701-5709 and 5721-5739, 28 U.S.C. 3101-3105, Debt Collection Act of 1982 (Pub. L. 97-365); 26 U.S.C. 6402(d); 31 U.S.C. 3711.

(i) The Federal Information Processing Standards (FIPS) 199 security impact category for the system is Moderate.

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

_____ This is a new information system.
_____ This is an existing information system with changes that create new privacy risks. *(Check all that apply.)*

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.
_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.

Section 2: Information in the System

2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated. *(Check all that apply.)*

Identifying Numbers (IN)					
a. Social Security*	X	e. File/Case ID		i. Credit Card	X[1]
b. Taxpayer ID	X	f. Driver's License		j. Financial Account	X
c. Employer ID	X	g. Passport		k. Financial Transaction	
d. Employee ID		h. Alien Registration		l. Vehicle Identifier	
m. Other identifying numbers (specify):					

*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form:

The Social Security Number is required to make payments to Federal employees, NIST associates, and sole proprietors through the Department of Treasury Bureau of Fiscal Services Payment Automation Manager (PAM). In addition, the Social Security Number is used to collect debts owed to NIST (i.e., overpayments for travel, salary, etc.) and other Government agencies as identified by the Department of Treasury Offset Program (TOPS).

[1] Government Purchase Cards, not personal credit cards.

General Personal Data (GPD)					
a. Name	X	g. Date of Birth		m. Religion	
b. Maiden Name		h. Place of Birth		n. Financial Information	X
c. Alias		i. Home Address	X	o. Medical Information	
d. Gender		j. Telephone Number	X	p. Military Service	
e. Age		k. Email Address	X	q. Physical Characteristics	
f. Race/Ethnicity		l. Education		r. Mother's Maiden Name	
s. Other general personal data (specify):					

Work-Related Data (WRD)					
a. Occupation	X	d. Telephone Number	X	g. Salary	X
b. Job Title		e. Email Address	X	h. Work History	
c. Work Address	X	f. Business Associates			
i. Other work-related data (specify):					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		d. Photographs		g. DNA Profiles	
b. Palm Prints		e. Scars, Marks, Tattoos		h. Retina/Iris Scans	
c. Voice Recording/Signatures		f. Vascular Scan		i. Dental Profile	
j. Other distinguishing features/biometrics (specify):					

System Administration/Audit Data (SAAD)					
a. User ID		c. Date/Time of Access		e. ID Files Accessed	
b. IP Address		d. Queries Run		f. Contents of Files	
g. Other system administration/audit data (specify):					

Other Information (specify)

2.2 Indicate sources of the PII/BII in the system. *(Check all that apply.)*

Directly from Individual about Whom the Information Pertains					
In Person	X*	Hard Copy: Mail/Fax	X*	Online	
Telephone	X*	Email			
Other (specify): *For purposes of invitational travel payment.					

Government Sources					
Within the Bureau	X	Other DOC Bureaus	X	Other Federal Agencies	X
State, Local, Tribal		Foreign			
Other (specify): General Service Administration System of Award Management (SAM) Department of Agriculture National Finance Center (NFC)					

Non-government Sources					
Public Organizations		Private Sector		Commercial Data Brokers	
Third Party Website or Application					
Other (specify):					

2.3 Describe how the accuracy of the information in the system is ensured.

The CBS/CFS accepts data from Government systems and supplements this data for payment and business related services provided via intergovernmental (Federal) shared services. Data is reviewed by the Federal Reserve, Department of Treasury, USDA, GSA, and NIST CBS/CFS managers for accuracy and completeness through business processes.

2.4 Is the information covered by the Paperwork Reduction Act?

	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection.
X	No, the information is not covered by the Paperwork Reduction Act.

2.5 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all that apply.)*

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)			
Smart Cards		Biometrics	
Caller-ID		Personal Identity Verification (PIV) Cards	
Other (specify):			

X	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.

Section 3: System Supported Activities

3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

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

X	There are not any IT system supported activities which raise privacy risks/concerns.

Section 4: Purpose of the System

4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated. *(Check all that apply.)*

Purpose			
For a Computer Matching Program		For administering human resources programs	
For administrative matters	X	To promote information sharing initiatives	
For litigation		For criminal law enforcement activities	
For civil enforcement activities		For intelligence activities	
To improve Federal services online		For employee or customer satisfaction	
For web measurement and customization technologies (single-session)		For web measurement and customization technologies (multi-session)	
Other (specify):			

Section 5: Use of the Information

5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

The CBS/CFS accepts data from Government systems and supplements this data for financial management and accounting purposes. The referenced general purpose data and work related data is in reference to employees, associates, invitational travelers, and vendors.

5.2 Describe any potential threats to privacy as a result of the bureau's/operating unit's use of the information, and controls that the bureau/operating unit has put into place to ensure

that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.)

Potential threats to privacy include the insider threat (e.g., authorized users misusing data or authorized user inadvertently combining multiple data sets resulting in aggregation of personal data). Information collected is directly from the vendor and is limited to only that which is needed for the service. Mitigating controls include employing and monitoring access, training for users and administrators, and assuring rules of behavior are agreed to by users.

Section 6: Information Sharing and Access

6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared. *(Check all that apply.)*

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau			X
DOC bureaus	X	X	X
Federal agencies		X	
State, local, tribal gov't agencies			
Public			
Private sector			
Foreign governments			
Foreign entities			
Other (specify):			

	The PII/BII in the system will not be shared.

6.2 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

X	Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage: The CBS/CFS receives input from components of the following information systems: 1. Department of Treasury Bureau of Fiscal Services (PAM and ASAP), 2. Department of Agriculture National Finance Center (NFC), and 3. NOAA1101, Information Technology Center (ITC) General Support System (GSS).
	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.3 Identify the class of users who will have access to the IT system and the PII/BII. *(Check all that apply.)*

Class of Users			
General Public		Government Employees	X
Contractors	X		
Other (specify):			

Section 7: Notice and Consent

7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. *(Check all that apply.)*

X	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement and/or privacy policy can be found at:	
X	Yes, notice is provided by other means.	Specify how: Disclose to invitational and relocation travelers that their information will be used for purposes of travel payments.
	No, notice is not provided.	Specify why not:

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

X	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how: An invitational traveler may decline to provide personal information and thus will not be eligible to travel on behalf of the Federal Government.
	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not:

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

X	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how: An invitational traveler consents to use for travel payment when providing personal information.
	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not:

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

X	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: An invitational traveler may update personal information through the initiator.
	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not:

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. *(Check all that apply.)*

	All users signed a confidentiality agreement or non-disclosure agreement.
X	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
X	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
X	Access to the PII/BII is restricted to authorized personnel only.
X	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: Access logs are kept and reviewed for anomalies on an as needed basis.
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): July 2, 2019 ☐ This is a new system. The A&A date will be provided when the A&A package is approved.
X	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
X	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POA&M).
X	A security assessment report has been reviewed for the supporting information system and it has been determined that there are no additional privacy risks.
X	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
	Contracts with customers establish ownership rights over data including PII/BII.
	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
	Other (specify):

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system. *(Include data encryption in transit and/or at rest, if applicable).*

The modules of the system are accessible on internal NIST networks protected by multiple layers of firewalls. Unauthorized use of the system is restricted by user authentication. Access logs are kept and reviewed for anomalies on an as needed basis. Data is stored on servers located at the NIST Gaithersburg, Maryland facility within the continental United States.

For information sharing, PII is transferred in a secure fashion. To guard against the interception of communication over the network, the components use the Transport layer Security (TLS) protocol which encrypts communications, or FIPS 140-2 encrypted virtual private network technologies between organizations. Access to CBS/CFS requires NIST-issued credentials because access is restricted by user authentication. NIST remote and other agency users access CBS/CFS on an authorized DOC network or connecting to the NIST network through a Virtual Private Network (VPN).

Section 9: Privacy Act

9.1 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*

As per the Privacy Act of 1974, "the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."

X	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name, number, and link. *(list all that apply)*: COMMERCE/DEPT-1, Attendance, Leave, and Payroll Records of Employees and Certain Other Persons COMMERCE/DEPT-2, Accounts Receivable COMMERCE/DEPT-9, Travel Records (Domestic and Foreign) of Employees and Certain Other Persons GSA/GOVT-4, Contracted Travel Services Program (E-Travel) GSA/GOVT-6, GSA SmartPay Purchase Charge Card Program GSA/GOVT-9, System for Award Management (SAM) GSA/GOVT-10, Federal Acquisition Regulation (FAR) Data Collection System
	Yes, a SORN has been submitted to the Department for approval on (date).
	No, this system is not a system of records and a SORN is not applicable.

Section 10: Retention of Information

10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. *(Check all that apply.)*

X	There is an approved record control schedule. Provide the name of the record control schedule: GRS 1.1 Financial Management and Reporting Records
	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
	Yes, retention is monitored for compliance to the schedule.
X	No, retention is not monitored for compliance to the schedule. Provide explanation: The CBS/CFS does not have the technical capabilities to archive/purge records.

10.2 Indicate the disposal method of the PII/BII. *(Check all that apply.)*

Disposal			
Shredding	X	Overwriting	
Degaussing		Deleting	
Other (specify): The CBS/CFS does not have the technical capabilities to archive/purge records.			

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Level

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed. *(The PII Confidentiality Impact Level is not the same as the Federal Information Processing Standards (FIPS) 199 security impact category.)*

	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
X	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

11.2 Indicate which factors were used to determine the above PII confidentiality impact levels. *(Check all that apply.)*

X	Identifiability	Provide explanation: The data types that are collected and maintained can be used to identify specific individuals.
X	Quantity of PII	Provide explanation: The quantity of PII that is collected and maintained pertains to employees, associates, and invitational travelers, from year 2000.
X	Data Field Sensitivity	Provide explanation: Includes general personal (e.g., social security number, financial, etc.) and work related data.
	Context of Use	Provide explanation:
X	Obligation to Protect Confidentiality	Provide explanation: The organization is legally obligated to protect the personal and business identifiable information within the financial applications.
X	Access to and Location of PII	Provide explanation: Data resides behind multiple layers of firewalls. Data is stored on servers which are within the continental United States.
	Other:	Provide explanation:

Section 12: Analysis

12.1 Identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Also, describe the choices that the bureau/operating unit made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data, include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

Potential threats to privacy include the insider threat (e.g., authorized users misusing data or authorized user inadvertently combining multiple data sets resulting in aggregation of personal data).

Information collected is directly from the employee and is limited to only that which is needed for the service. Mitigating controls include employing and monitoring administrative access, training for administrators, and assurance of rules of behavior.

12.2 Indicate whether the conduct of this PIA results in any required business process changes.

	Yes, the conduct of this PIA results in required business process changes. Explanation:
X	No, the conduct of this PIA does not result in any required business process changes.

12.3 Indicate whether the conduct of this PIA results in any required technology changes.

	Yes, the conduct of this PIA results in required technology changes. Explanation:
X	No, the conduct of this PIA does not result in any required technology changes.