Template Version Number: 01-2022

U.S. Department of Commerce
National Technical Information Service
(NTIS)

Privacy Impact Assessment
for the
NTIS Financial Systems

Reviewed by: Bilal Baisa, Bureau Chief Privacy Officer (BCPO)

☐ Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
☐ Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
☒ Concurrence of the BCPO (This is an existing information system that is eligible for an annual certification)

Tahira Murphy 6/30/2023

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer Date
(Or the BCPO if this is an existing system that is eligible for an annual certification)

U.S. Department of Commerce Privacy Impact Assessment
NTIS/NTIS Financial Systems (NTIS 002)

Unique Project Identifier: CSAM ID – 2525

Introduction: System Description

Provide a brief description of the information system.

The NTIS Financial System (NTIS002) is the collection of major application that are hosted on NTIS servers located at the NTIS Data Center (5301 Shawnee Rd, Alexandria, VA 22312) and in AWS Cloud. These systems work together to allow NTIS to provide services and process finances for the general public, as well as internally. All products and services sold by NTIS are processed by the NTIS002 Information System. The Federal Information Processing Standards (FIPS) 199 security impact category for the system is Moderate. NTIS002 utilizes the following major applications to achieve the NTIS mission; Budget Accounting Purchasing System (BAPS), Financial Reporting System (FRS), Cost Perform, ELAN, and a PAY.gov Client. These Major Applications work in hand to collect, process, and disseminate information across the NTIS002 system.

BAPS is designed to provide agency funds control, support and documentation for all of the agency expenditures, obligations, accruals, undelivered orders, accounts payable, advances to others, and disbursements, as well as audit documentation for NTIS. This system is used by NTIS employees in the offices of Business & Development and Budget & Accounting. Agency purchase requests are entered into BAPS which will then appropriately obligate funds or accruals. The system then waits for a vendor invoice which will require approval from NTIS staff. Once invoices are approved, payments are processed out-of-band by a US Treasury system and contract award information is then recorded back in BAPS.

The FRS application is used by NTIS Budgeting & Accounting. It consists of several Access Databases to include, labor, allocations, planning, ELAN input (order processing system), contractor labor, revenue, unit sales and some smaller Microsoft Access Databases (MDB). The areas of interest for reporting provides each director and section managers with data needed for their section's business. (Costs, performance, revenue, budgeting, etc.). FRS combines data from the National Finance Center (NFC) Payroll System (manually imported), BAPS non-labor data, revenue planning, product revenue, and unit sales from ELAN. Using this data, FRS calculates and distributes NTIS' overhead to all products and services, calculates and distributes all NTIS allocated costs for local overhead and other allocated functions (customer service, product distribution, product management, sales desk, etc.) to all products and services, calculates revenue charged to service clients based on their agreement terms and combines all of this data to report revenue, cost and net by products and/or service products.

Cost Perform is a system utilized by NTIS employees in the offices of Business & Development and Budget & Accounting to determine and allocate agency overhead costs. Cost Perform utilizes data from BAPS and FRS to determine accurate agency overheads costs for planning and evaluation.

ELAN and PAY.gov Client are utilized to process the payments received by NTIS002. ELAN encrypts credit card data from transactions and sends the info to the PAY.gov Client, which returns a transaction ID. The transaction ID and the last 4 digits of the credit card are stored in the system. The PAY.gov Client validates or charges credit card, using the encrypted information from ELAN, through PAY.gov. The two web services communicate with each other in order to fully process a payment through PAY.gov.

NTIS002 collects information from all individuals who order and/or purchase products and services from NTIS and all individuals who have requested to be placed on the NTIS promotional literature mailing list. Information sharing across the NTIS002 subsystems include the following categories of data.

This information includes name; address; nine-digit taxpayer identification number; items ordered; items sent; amount of purchases, date order received; date order mailed; NTIS deposit account or customer code number; total charge to date; whether account collectible or not; categories of publications ordered by each purchaser; when subscription expired; ELAN stores the last 4 digits of the credit card only; FRS has the individual salary and pay grades and correlates it to their name.

The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information is 15 U.S.C. 1151–57; 41 U.S.C. 104, 44 U.S.C. 3101.

Address the following elements:

(a) Whether it is a general support system, major application, or other type of system
NTIS 002 Financial Systems is a major application.

(b) System location
The NTIS Business System (NTIS002) is the collection of major applications that are hosted on NTIS servers located at the NTIS Data Center (BAPS, FRS, & Cost Perform) and in AWS Cloud US East Region and AWS Cloud US West Region (ELAN and Pay.gov).

(c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)
BAPS is interconnected with FRS. FRS is interconnected with Cost Perform. ELAN is interconnected with Pay.gov. The FRS system is designed to connect with ELAN to process financial transactions and send it to the BAPS Access database for transactional record retention.

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

BAPS is designed to provide agency funds control, support and documentation for all of the agency expenditures, obligations, accruals, undelivered orders, accounts payable, advances to others, and disbursements, as well as audit documentation for NTIS. This system is used by NTIS employees in the offices of Business & Development and Budget & Accounting. Agency purchase requests are entered into BAPS which will then appropriately obligate funds or accruals. The system then waits for a vendor invoice which will require approval from NTIS staff. Once invoices are approved, payments are processed out-of-band by a US Treasury system and contract award information is then recorded back in BAPS.

The FRS application is used by NTIS Budgeting & Accounting. It consists of several Access Databases to include, labor, allocations, planning, ELAN input (order processing system), contractor labor, revenue, unit sales and some smaller Microsoft Access Databases (MDB). The areas of interest for reporting provides each director and section managers with data needed for their section's business. (Costs, performance, revenue, budgeting, etc.). FRS combines data from the National Finance Center (NFC) Payroll System (manually imported), BAPS non-labor data, revenue planning, product revenue, and unit sales from ELAN. Using this data, FRS calculates and distributes NTIS' overhead to all products and services, calculates and distributes all NTIS allocated costs for local overhead and other allocated functions (customer service, product distribution, product management, sales desk, etc.) to all products and services, calculates revenue charged to service clients based on their agreement terms and combines all of this data to report revenue, cost and net by products and/or service products.

Cost Perform is a system utilized by NTIS employees in the offices of Business & Development and Budget & Accounting to determine and allocate agency overhead costs. Cost Perform utilizes data from BAPS and FRS to determine accurate agency overheads costs for planning and evaluation.

ELAN and PAY.gov Client are utilized to process the payments received by NTIS002. ELAN encrypts credit card data from transactions and sends the info to the PAY.gov Client, which returns a transaction ID. The transaction ID and the last 4 digits of the credit card are stored in the system. The PAY.gov Client validates or charges credit card, using the encrypted information from ELAN, through PAY.gov. The two web services communicate with each other in order to fully process a payment through PAY.gov.

(e) How information in the system is retrieved by the user

BAPS does not have any non-organizational users that authenticate to the system. Organizational users authenticate through multiple levels including, PIV Windows authentication, Open Database Connectivity (ODBC), and application log in. Application log-in is controlled by Active Directory credentials.

Users authenticate to the ELAN web interface with a username and password created by the ELAN web application administrator. ELAN's web application user level of access is locally defined per NTIS roles.

For Pay.gov only System Administrators authenticate to the system using local credentials, username and password, assigned by the application administrator. PAY.gov Client is a web service located in NTIS internal system. Users cannot directly connect to the PAY.gov Client. This system is not a web-based application; therefore, users do not access this application through a URL.
FRS does not have any non-organizational users that authenticate to the system. Organizational users authenticate through multiple levels including; PIV-required Windows workstation authentication, ODBC, and manual Access Database log-in (only applicable to older versions of Windows OS).

(f) How information is transmitted to and from the system
Transactions between PAY.gov and PAY.gov Client is through a custom TLS 1.2 certificate that PAY.gov generates based on the client information, such as IP address. The NTIS public IP for PAY.gov Client is added to the PAY.gov IP whitelist. Without the certificate, connections are automatically rejected during the HTTPS/TLS 1.2 handshake process. This certificate is renewed or changed every three (3) years to maintain a secure connection. ELAN connects to PAY.gov Client through the internal ELAN ECP Gateway Proxy via HTTPS/TLS 1.2.

FRS does not utilize any external interfaces. FRS interfaces and connects internally with BAPS. All information entered into BAPS is done manually and does not have any automated processes that interact with any other systems.

(g) Any information sharing
NTIS Business Systems does not share any information.

(h) The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information
The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information is 15 U.S.C. 1151–57; 41 U.S.C. 104, 44 U.S.C. 3101.

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

____ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment.

_X__ This is an existing information system that is eligible for an annual certification, in which security and privacy controls are properly implemented, 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*		f. Driver's License		j. Financial Account	X
b. Taxpayer ID	X	g. Passport		k. Financial Transaction	X
c. Employer ID	X	h. Alien Registration		l. Vehicle Identifier	
d. Employee ID	X	i. Credit Card	X	m. Medical Record	
e. File/Case ID					
n. Other identifying numbers (specify):					
*Explanation for the business need to collect, maintain, or disseminate the Social Security number, including truncated form:					

General Personal Data (GPD)					
a. Name	X	h. Date of Birth		o. Financial Information	X
b. Maiden Name		i. Place of Birth		p. Medical Information	

General Personal Data (GPD)					
c. Alias		j. Home Address	X	q. Military Service	
d. Gender		k. Telephone Number	X	r. Criminal Record	
e. Age		l. Email Address	X	s. Marital Status	
f. Race/Ethnicity		m. Education		t. Mother's Maiden Name	
g. Citizenship		n. Religion			
u. Other general personal data (specify): Financial Transaction					

Work-Related Data (WRD)					
a. Occupation	X	e. Work Email Address		i. Business Associates	
b. Job Title	X	f. Salary	X	j. Proprietary or Business Information	
c. Work Address		g. Work History		k. Procurement/contracting records	
d. Work Telephone Number		h. Employment Performance Ratings or other Performance Information			
l. Other work-related data (specify):					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		f. Scars, Marks, Tattoos		k. Signatures	
b. Palm Prints		g. Hair Color		l. Vascular Scans	
c. Voice/Audio Recording		h. Eye Color		m. DNA Sample or Profile	
d. Video Recording		i. Height		n. Retina/Iris Scans	
e. Photographs		j. Weight		o. Dental Profile	
p. 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		f. 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		Hard Copy: Mail/Fax	X	Online	
Telephone	X	Email			
Other (specify):					

Government Sources					
Within the Bureau	X	Other DOC Bureaus		Other Federal Agencies	

Government Sources					
State, Local, Tribal		Foreign			
Other (specify):					

Non-government Sources					
Public Organizations	X	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.

All sensitive data at rest in the NTIS002 subsystems are encrypted using AES-256 encryption technology. To ensure system information is not modified or changed, the relevant NTIS002 databases through utilization of integrity checking functions and hashes for each record.

Any hardcopies of data files on NTIS staff and employees are stored in locked cabinet in a locked office within the NTIS financial department for which only authorized individuals are allowed access.

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	X
For litigation		For criminal law enforcement activities	
For civil enforcement activities		For intelligence activities	
To improve Federal services online	X	For employee or customer satisfaction	X
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).

PII Data within the NTIS002 Information System is collected from several different sources; Taxpayer ID, Employer ID, Employee ID, Name, Address, Telephone Number, Email Address, Financial Information, occupation, Job Title, and Salary are collected directly from the individual through Hard Copy, Telephone, or through an Online portal. This information is used by NTIS002 to process financial reimbursement to federal employees.

Taxpayer ID, Employer ID, Credit Card, Financial Account, Financial Transaction, and Financial Information are collected from Within the Bureau, Other DOC Bureaus, and Public Organizations. This information I used by NTIS002 to process payments for products and services offered by NTIS.

5.2 Describe any potential threats to privacy, such as insider threat, 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.)

Threats to privacy for NTIS002 are minimized by the controls deployed to protect information at rest and in transit. All NTIS002 sub-systems utilize the latest cryptographic technologies and methods such as TLS 1.2 (HTTPS) for data in transit, and AES-256 encryption for data at rest. All physical copies of information that need to be disposed are shredded, and legacy hard drives are physically destroyed. Financial documentation that is stored as the original hardcopies are kept in a locked cabinet, within a locked and secured office within the financial department to which only authorized individuals are allowed access.

NTIS combats the potential for Insider Threat through on-going training exercises, such as Phishing Initiatives, Departmental Annual Security and Privacy Awareness Training, and on-going newsletters and email alerts sent to NTIS Staff. Accounts are reviewed on a quarterly basis to ensure stale accounts and accounts that are no longer needed are removed and inaccessible.

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			

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
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 Does the DOC bureau/operating unit place a limitation on re-dissemination of PII/BII shared with external agencies/entities?

	Yes, the external agency/entity is required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
	No, the external agency/entity is not required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
X	No, the bureau/operating unit does not share PII/BII with external agencies/entities.

6.3 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: Elan connects to Pay.gov via a client terminal service is encrypted via HTTPS TLS v1.2. In addition, Pay.gov has specifically IP white listed the pay.gov client (part of Elan).
	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.4 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

Class of Users			
Contractors			
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.	
X	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: https://www.osec.doc.gov/opog/PrivacyAct/PrivacyAct.html	
	Yes, notice is provided by other means.	Specify how:
	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: If individuals wish to decline to provide PII/BII they must opt out of using the system. Orders cannot be processed if information is not provided.
	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: The NTIS Privacy policy states "If you purchase a product on-line, we collect personal information required to support the purchasing of products, including names, addresses, telephone and fax numbers and e-mail addresses"
	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: Individuals may request to review/update their PII/BII by email or calling the NTIS Office of Financial Management.
	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.)*

X	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: All access to the systems are logged, monitored, tracked, recorded via the NTIS SIEM tool and reviewed in real time by the ESOC Team.
X	The information is secured in accordance with the Federal Information Security Modernization Act (FISMA) requirements. Provide date of most recent Assessment and Authorization (A&A): 07/22/2022 ☐ 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 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 DOC 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).*

All NTIS002 sub-systems utilize the latest cryptographic technologies and methods such as TLS 1.2 (HTTPS) for data in transit, and AES-256 encryption for data at rest.

All physical copies of information that need to be disposed are shredded, and legacy hard drives are physically destroyed. Financial documentation that is stored as the original hardcopies are kept in a locked cabinet, within a locked and secured office within the financial department to which only authorized individuals are allowed access. Additionally, all NTIS staff participate in mandatory security training annually.

All NTIS002 systems are monitored via the robust measures of the NTIS SIEM and reviewed in real time by the ESOC team.

Section 9: Privacy Act

9.1 Is the PII/BII searchable by a personal identifier (e.g, name or Social Security number)?

__X__ Yes, the PII/BII is searchable by a personal identifier.

____ No, the PII/BII is not searchable by a personal identifier.

9.2 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/NTIS-1 COMMERCE/DEPT-1 COMMERCE/DEPT-18 COMMERCE/DEPT-2 COMMERCE/DEPT-9 COMMERCE/DEPT-23
	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: NC1-422-82-01 National Technical Information
	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:

X	Yes, retention is monitored for compliance to the schedule.
	No, retention is not monitored for compliance to the schedule. Provide explanation:

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

Disposal			
Shredding	X	Overwriting	X
Degaussing		Deleting	X
Other (specify):			

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, and does not have to be 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.
X	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
	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 level. *(Check all that apply.)*

X	Identifiability	Provide explanation: The system specifically identifies individuals using their first and last names, employee ID, financial information, contact information (address, telephone number, email, and work-related data (occupation, job title, salary).
X	Quantity of PII	Provide explanation: NTIS002 collects financial information only from individuals/companies who order and/or purchase products and services from NTIS. These individuals/companies provide payment information after initiating a request to receive a product or service from NTIS. Most of the customers of NTIS are institutions, i.e. Credit companies, Banks, Health Organizations, Local Governments, etc.
X	Data Field Sensitivity	Provide explanation: Hard copy forms have PII information, such as Name, Address, Financial Information, etc. Online forms can contain PII information, such as Financial Transaction Information, Employer ID, Employee ID, etc.

X	Context of Use	Provide explanation: The PII within the system is collected, stored, used, processed, disclosed, or disseminated to support authentication of employee identity and tracking of financial transaction records of requesting individuals/companies. Financial information is ONLY collected for individuals/companies that have initiated a request to access the products/services offered by NTIS.
	Obligation to Protect Confidentiality	Provide explanation:
X	Access to and Location of PII	Provide explanation: The hard copies of employee financial information are stored in a locked file cabinet, and only made available to personnel deemed to have a job responsibility to access the information to complete a business function. Access to PII online is secured by cryptographic technologies and methods such as TLS 1.2 (HTTPS) for data in transit, and AES-256 encryption for data at rest.
	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.)

There are no significant threats to privacy given the current architecture and implementation of electronic system components. NTIS implemented the system in a manner which does not electronically store sensitive PII such as social security numbers or account information. Works flows and processes are structured in a manner to process payments to staff and vendors without actually storing sensitive data on the system, NTIS financial staff will process payments out-of-band through a US Treasury system and then utilize NTIS002 system for tracking and accounting using non sensitive identifiers. Additional any data collection is designed to only capture the minimal amount of information necessary to achieve the functions of the system.

The most significant threat to privacy for this system would be to loss of paper records via theft. This risk is mitigated by the use of strong physical controls including, surveillance systems, monitored keycard access to secured areas, security doors and locks implemented strategically to deter and prevent unauthorized physical access, and ensuring only authorized financial staff have access to the relevant paper records stored in locked cabinets in a single locked room in the financial department.

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.