Template Version Number: 01-2022

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

Privacy Threshold Analysis
for the
NTIS Financial Systems

U.S. Department of Commerce Privacy Threshold Analysis

NTIS/NTIS Financial Systems (NTIS 002)

Unique Project Identifier: CSAM ID – 2525

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 on 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: *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).

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 purpose that the system is designed to serve*
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.

e) *The way the system operates to achieve the purpose*
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.

f) A general description of the type of information collected, maintained, used, or disseminated by the system

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.

g) Identify individuals who have access to information on the system

The system will have internal system users, system administrators, and system developers.

h) 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).

i) How information is transmitted to and from the system

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.

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.

Questionnaire:

1. Status of the Information System

1a. 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	

Changes That Create New Privacy Risks (CTCNPR)					
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. *Continue to answer questions and complete certification.*

__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. *Skip questions and complete certification.*

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

____ Yes. This is a new information system.

____ Yes. This is an existing information system for which an amended contract is needed.

____ No. The IT Compliance in Acquisitions Checklist is not required for the acquisition of equipment for specialized Research and Development or scientific purposes that are not a National Security System.

_X__ 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.

____ Yes. *(Check all that apply.)*

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

_X__ 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.)."

_X__ Yes, the IT system collects, maintains, or disseminates BII.

____ No, this IT system does not collect any BII.

4. Personally Identifiable Information (PII)

4a. Does the IT system collect, maintain, or disseminate 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."

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

__X__ DOC employees
__X__ Contractors working on behalf of DOC
____ Other Federal Government personnel
_X___ 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 Social Security numbers (SSNs), including truncated form?

____ Yes, the IT system collects, maintains, or disseminates 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.

_X___ No, the IT system does not collect, maintain, or disseminate SSNs, including truncated form.

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

__X__ 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.

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.

____ Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

__X__ 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, 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.

CERTIFICATION

__X__ The criteria implied by one or more of the questions above **apply** to the NTIS Financial Systems 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 [IT SYSTEM NAME] and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

System Owner Name: Leigh Anne Levesque Office: NTIS/OCIO Phone: 703-605-6097 Email: LLevesque@ntis.gov Signature: Leigh Anne Levesque Digitally signed by Leigh Anne Levesque Date: 2023.05.08 09:18:24 -04'00' Date signed: _____	**Information Technology Security Officer** Name: Bilal Baisa Office: OCIO Phone: 703-605-6172 Email: bbaisa@ntis.gov Signature: Bilal Baisa Digitally signed by Bilal Baisa Date: 2023.04.12 11:54:13 -04'00' Date signed: _____
Privacy Act Officer Name: Bilal Baisa Office: OCIO Phone: 703-605-6172 Email: bbaisa@ntis.gov Signature: Bilal Baisa Digitally signed by Bilal Baisa Date: 2023.04.12 11:54:29 -04'00' Date signed: _____	**Authorizing Official** Name: Wayne Strickland Office: NTIS/OCIO Phone: 703-605-6543 Email: wstrickland@ntis.gov Signature: Wayne Strickland Digitally signed by Wayne Strickland Date: 2023.05.18 15:00:19 -04'00' Date signed: _____
Bureau Chief Privacy Officer Name: Bilal Baisa Office: OCIO Phone: 703-605-6172 Email: bbaisa@ntis.gov Signature: Bilal Baisa Digitally signed by Bilal Baisa Date: 2023.04.12 11:55:34 -04'00' Date signed: _____	

This page is for internal routing purposes and documentation of approvals. Upon final approval, this page must be removed prior to publication of the PTA.