

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



**Privacy Impact Assessment
for the
Office of Data and Informatics e-Commerce System (641-01)**

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

CATRINA PURVIS

Digitally signed by CATRINA PURVIS
DN: c=US, o=U.S. Government, ou=Department of Commerce, ou=Office of the
Secretary, cn=CATRINA PURVIS, 0.9.2342.19200300.100.1.1=13001002875743
Date: 2018.09.28 18:55:21 -04'00'

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: 641-01

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.

(a) a general description of the information in the system

The Office of Data and Informatics e-Commerce system permits the sale of informatic reference materials to the public. The system permits inventory, order, and purchase of materials by the public, with backend processes to the internal financial system, and connectivity to pay.gov.

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

(b) a description of a typical transaction conducted on the system

The programmatic function collects PII and BII as a point of sale function for the public to purchase informatics reference material. Public purchase may be from an individual consumer or business.

(c) any information sharing conducted by the system

The system shares information with other internal NIST business units, and pay.gov.

(d) a citation of the legal authority to collect PII and/or BII

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 275) 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); and 31 U.S.C. 3711.

(e) the Federal Information Processing Standard (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): None				

This is an existing information system in which changes do not create new privacy risks.

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*		e. File/Case ID		i. Credit Card
b. Taxpayer ID	X ¹	f. Driver's License		j. Financial Account
c. Employer ID		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:

¹A Taxpayer Identification Number (TIN) is an identification number used by the Internal Revenue Service (IRS) in the administration of tax laws. It is issued either by the Social Security Administration (SSA) or by the IRS. A Social Security number (SSN) is issued by the SSA whereas all other TINs are issued by the IRS.

General Personal Data (GPD)				
a. Name	X	g. Date of Birth		m. Religion
b. Maiden Name		h. Place of Birth		n. Financial Information
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		d. Telephone Number	X	g. Salary

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): None					

System Administration/Audit Data (SAAD)					
a. User ID	X	c. Date/Time of Access	X	e. ID Files Accessed	
b. IP Address	X	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	X
Telephone	X	Email	X		
Other (specify):					

Government Sources					
Within the Bureau		Other DOC Bureaus		Other Federal Agencies	
State, Local, Tribal		Foreign			
Other (specify):					

Non-government Sources					
Public Organizations		Private Sector		Commercial Data Brokers	
Third Party Website or Application					
Other (specify): None					

2.3 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):

<input checked="" type="checkbox"/> 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	<input checked="" type="checkbox"/>
Other (specify):			

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			
To determine eligibility		For administering human resources programs	
For administrative matters	<input checked="" type="checkbox"/>	To promote information sharing initiatives	
For litigation		For criminal law enforcement activities	
For civil enforcement activities		For intelligence activities	
To improve Federal services online	<input checked="" type="checkbox"/>	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).

SRD customers are foreign and domestic individuals, companies, and academic institutions. The SRD sales information is primarily transaction based including the products ordered, who ordered them, and how they were delivered. This information is collected to complete an electronic commerce transaction. SRD sales information in the form of unit sales self-reported to NIST by existing distributor is also stored. This information is collected to process checks, wire transfers and generate NIST forms required by accounting. Information is primarily entered by the customer when purchasing a standard reference data product, for example all the information needed to process a credit card for billing and shipping.

For paying customers of SRD products that are eligible for free upgrades, this information is used to contact customers to offer free product updates.

For SRD distributors, this information is used to contact distributors on a regular basis to re-sign agreements, or troubleshoot royalty reporting issues.

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	X	X
DOC bureaus			
Federal agencies			
State, local, tribal gov't agencies			
Public			
Private sector			
Foreign governments			
Foreign entities			
Other (specify):			

This information is not shared, customer service representatives directly access the data.

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	<p>Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII.</p> <p>The system connects with the NIST 162-01 Commerce Business System, Core Financial System (CBS/CFS), and directly with pay.gov for credit card purchases.</p>
	<p>No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.</p>

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	
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 Policy can be found at: https://www.nist.gov/policies-notices . A Privacy Act Statement is found when customer's place orders through the online order form, initiated from: https://www.nist.gov/srd/purchase-srd	
	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: Individuals choose whether to place an order or request a service. In order to initiate the order or service, PII/BII must be provided. The individual can choose to decline to provide PII/BII and not complete an order or request a service.
	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.

	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how:
X	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not: If an individual chooses to provide their PII/BII for an order or to request a service, there is no additional consent requested of that individual for particular uses of their PII/BII.

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 have opportunity to review/update their PII/BII at any point during the ordering process.
	No, individuals do not have an opportunity to review/update PII/BII	Specify why not:

	pertaining to them.	
--	---------------------	--

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.
	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
	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 to PII/BII is logged in the appropriate system logs.
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): October 23, 2017 <input type="checkbox"/> 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 (POAM).
	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.

The applications 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/BII 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 and the public. Internal access to the applications require NIST-issued credentials because access is restricted by user authentication.

Access to the administration interface is secured with SSL. Access to the administrative interface is limited by IP address, only authorized systems in Gaithersburg can login. Access to the administrative interface is restricted by username and password. All transactions are logged. No credit card information is stored in the system.

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.”

<input checked="" type="checkbox"/>	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name and number <i>(list all that apply)</i> :
	COMMERCE/DEPT-2, Accounts Receivable
	Yes, a SORN has been submitted to the Department for approval on <u>(date)</u> .
	No, a SORN is not being created.

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.)*

<input checked="" type="checkbox"/>	There is an approved record control schedule. Provide the name of the record control schedule: NIST Comprehensive Records Schedule Item 31 (maintains standard reference material 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:
<input checked="" type="checkbox"/>	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	<input checked="" type="checkbox"/>	Overwriting	
Degaussing		Deleting	<input checked="" type="checkbox"/>
Other (specify): Only non-record data is being destroyed by shredding and deleting.			

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

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.

	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 levels.
(Check all that apply.)

	Identifiability	Provide explanation:
X	Quantity of PII	Provide explanation: Collection of TaxID, Credit Card, and Financial Account. A Taxpayer Identification Number (TIN) is an identification number used by the Internal Revenue Service (IRS) in the administration of tax laws. It is issued either by the Social Security Administration (SSA) or by the IRS. A Social Security number (SSN) is issued by the SSA whereas all other TINs are issued by the IRS.
	Data Field Sensitivity	Provide explanation:
	Context of Use	Provide explanation:
	Obligation to Protect Confidentiality	Provide explanation:
	Access to and Location of PII	Provide explanation:
	Other:	Provide explanation:

Section 12: Analysis

12.1 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.

12.2 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.