Template Version Number: 01-2021

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

Privacy Impact Assessment
for the
138-01 Business Operations Office (BOO) System

Reviewed by: Claire Barrett, 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

CLAIRE BARRETT Digitally signed by CLAIRE BARRETT
Date: 2022.05.31 21:42:18 -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: 138-01

Introduction: System Description

Provide a brief description of the information system:
(a) Whether it is a general support system, major application, or other type of system
(b) System location
(c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)
(d) The way the system operates to achieve the purpose(s) identified in Section 4
(e) How information in the system is retrieved by the user
(f) How information is transmitted to and from the system
(g) Any information sharing
(h) The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information
(i) The Federal Information Processing Standards (FIPS) 199 security impact category for the system

The NIST Business Operations Office (BOO) system is used to implement an enterprise-level Customer Relationship Management (CRM) system so that NIST organizations can manage interactions and relationships with customers while also offering an online storefront to sell NIST products and services to the public.

The Salesforce application is owned by the Business Operations Office (BOO) which is part of Management Resources organization at NIST. Implementation of Salesforce is the responsibility of NIST 188-01 – Platform Services Division. The various OUs that use Salesforce own the data associated with the respective implementations.

a. Whether it is a general support system, major application, or other type of system
This is a general support system.

b. System location
The system is located at the NIST facility in Gaithersburg, MD while the cloud-based components are located in San Francisco, California.

c. Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)
System interconnects with NIST 188-01, NIST 162-01, and NIST 640-01.

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

BOO's vision is to fulfill its mission to deliver exceptional products and services using project management, process engineering, relationship management, and customer engagement as follows:

CRM - BOO works with stakeholders across NIST to provide an enhanced understanding of how NIST interacts with customers and partners.

The CRM system will provide NIST with customer and business information about how NIST provides products, services and any related inquires. CRM data will be collected and entered by NIST OU users and will contain customer PII and BII. This instance (https://nist.my.salesforce.com) also contains a Maintenance and Operation module which is used by the NIST CRM vendor to provide helpdesk support to NIST users.

Information is obtained by the public who are reaching out to NIST for NIST products and service. All data is non-sensitive customer email and contact information copied by NIST staff from Microsoft Office 365, or entered via a public facing form (https://www.nist.gov/about-nist/contact-us).

E-Commerce - BOO leads the effort to improve how NIST transactions take place. They do this by implementing and managing an e-commerce platform that allows customers to place online orders while they manage invoice and payment processes.

E-Commerce includes a web-based storefront (https://shop.nist.gov) that allows customers to view and purchase products in the NIST catalog. After creating an account, customers can make purchases, retrieve order history, status, invoices/receipts, and self-service their data and passwords. User account data includes customers name, address, and e-mail. Customers can pay for services using checks, wire transfers, purchase orders, Intra-governmental Payment and Collection (IPAC), and the Pay.gov payment service. The storefront has been customized for NIST, and information is generated in the cloud.

E-Commerce will also use an externally hosted application, DocuSign. The application will be used to obtain signatures from both internal NIST users as well as external customers. Signatures will be generated on various product and service reports, distributor agreements, and site license orders as well as NIST return shipping forms (NIST 64). These services will be used by Calibrations, Standard Reference Data (SRD), Standard Reference Materials (SRM), and Standard Reference Instruments (SRI).

e. How information in the system is retrieved by the user

CRM data is accessed directly through the component by authorized NIST users. Role-based permissions are used.

E-Commerce data is also accessed directly through the component via navigation from nist.gov or shop.nist.gov URLs. Then after customers have created an account, they can sign in to make a purchase. When a customer creates an account, they will enter name, address, and email which will be generated in the Salesforce cloud. Once they have an account, they will be able to retrieve their order history, status, invoices/receipts, and self-service their data and passwords. Internal NIST end users who support the customers on this system must access the backend system behind the NIST firewall and access must go through the SSO.

After a customer places an order within the system, administrators fulfill the order and prepare for shipping. Customers will then receive an email with a link to download the products. E-Commerce customer service agents use an internal portal to manage customer orders and to provide customer service.

f. How information is transmitted to and from the system

All system connectivity is via TCP/IP across the NIST Network Infrastructure (SSP 181-04). The NIST Network Infrastructure system provides all services for physical cabling, network frame synchronization/ flow control/ error checking, routing, switching, and DNS.

Remote connections to NIST internal resources (i.e. telecommuting, travel, etc.) are made via SSL Remote Access services managed as part of the NIST Network Security system (SSP 181-01).

g. Any information sharing conducted by the system

E-Commerce has integrations with other entities and third-party systems to carry out specific functions to complete and record customer transactions. These include:

1. **Pay.Gov (Treasury) – Salesforce submits order details to Pay.gov to process electronic credit card payments via webservices. E-Commerce uses Hosted Collection Pages Service (HCPS), which is part of Trusted Computing Services suite. E-Commerce does not store or track customer payment information.**
2. **Commerce Business System/Commerce Financial System (NIST 162-01) - Accounts receivable files and billing invoice files are produced from Salesforce B2B and manually downloaded from the Salesforce Cloud. Files are then saved onto a user's secure network, and then uploaded to the CBS database server via chron job. Payment transactions are also provided by Treasury to be uploaded to CBS, but this activity takes place outside of the Salesforce environment.**
3. **DocuSign – Used to obtain electronic signatures from customers as well as NIST users on various reports generated through the NIST storefront.**
4. **Limestone application (NIST 640-01) - An internal web-based application to generate the PDFs required for customers such as invoices, quotes, and receipts. In Phase 1, Limestone will generate: perform invoice, quote and receipt. Phase 2 will expand this feature.**

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.

Public Law 90-396, July 11, 1968, The Standard Reference Data Act;

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.

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 an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2017 or later).

Changes That Create New Privacy Risks (CTCNPR)
Other changes that 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)
Other identifying numbers:
Explanation for the business need to collect, maintain, or disseminate the Social Security number, including truncated form:

General Personal Data (GPD)
Name **Home Address** **Telephone Number** **Email Address**
Other general personal data:

Work-Related Data (WRD)
Occupation **Job Title** **Work Address**

Work Telephone Number **Work Email Address** **Business Associates** **Proprietary or Business Information**
Other work-related data:

Distinguishing Features/Biometrics (DFB)
Other distinguishing features/biometrics:

System Administration/Audit Data (SAAD)
User ID **IP Address** **Date/Time of Access**
Other system administration/audit data:

Other Information

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 **Telephone** **Hard Copy - Mail/Fax** **Email** **Online**
Other:

Government Sources
Other:

Non-government Sources
Other:

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

Accuracy is ensured in CRM because data is collected directly from the user. If data needs to be corrected or updated, an individual may contact their NIST point of contact.

The NIST Storefront collects customer data directly from users (i.e., public customers), and users can review/update their profile through the online portal at any time. Data is also reviewed by NIST staff to ensure fulfillment of the order. Once completed, the orders are then sent to either Pay.gov or NIST 162-01 for payment. Notifications will be sent to users to confirm successful payment.

If a signature is required for a transaction, signatures and documents are uploaded, encrypted, and a unique hash is created. If a signed document has been tampered with or compromised, the hash will not match the digital signature information. **NIST 188-01 infrastructure maintains controls (e.g., encryption at rest and encryption in transit) to ensure the data cannot be altered by unauthorized persons.**

2.4 Is the information covered by the Paperwork Reduction Act?

No, the information is not covered by the Paperwork Reduction Act.
The OMB control number and the agency number for the collection:

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

No

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)
Other:

Section 3: System Supported Activities

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

No

The IT system supported activities which raise privacy risks/concerns.

Activities
Other:

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 administrative matters **To improve Federal services online** **For employee or customer satisfaction**
Other:

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).

CRM: Business contact information will be used to better integrate and communicate with various business communities. CRM enables NIST to centralize and aggregate data regarding its customer base and their interest areas, permitting insight into interactions and relationships with a customer and/or business. In turn, NIST is able to better understand customer needs. CRM also allows NIST to automate its workflows, allowing insight into the status of Cooperative Research and Development Agreements (CRADAs). The PII/BII in the CRM may be about federal employees, federal contractors, foreign nationals, members of the public, or partners and stakeholders.

E-Commerce: Scientific and technology related sales take place via the E-Commerce component, and PII is be used to facilitate that process.

The redress of customer's information will be mostly self-serviced by the customer. Additionally, contact information (names/emails/phone numbers) will be provided for customers to directly contact someone at NIST to update their information if they run into a problem or have a request they cannot perform themselves.

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.)

CRM: Salesforce has an approval process used before sharing data. Salesforce also takes advantage of contractual clauses and Rules of Behavior. Cloud activity can mean some limited risk.

E-Commerce: Activity does not present significant risk and has its own Rules of Behavior form for internal users to sign before obtaining access.

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 customer 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 compliance to records management schedules. Information system security controls used to protect this information are implemented, validated, and continuously monitored.

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.)*

Yes, the PII/BII in the system will be shared

The recipients the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared.

Bulk Transfer - Within the bureau **Case-by-Case - Federal Agencies** **Case-by-Case - Within the bureau** **Direct Access - Within the bureau** **Other**
Other:

Case-by-Case - Federal Agencies – (Treasury (pay.gov) used for payments) **Case-by-Case - Within the bureau - (162-01 used for payments)** **Direct Access - Within the bureau - (188-01 for platform services, 640-01 for use of Limestone)**

6.2 Does the DOC bureau/operating unit place a limitation on re-dissemination of PII/BII shared with external agencies/entities?

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

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

Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII.
The name of the IT system and description of the technical controls which prevent PII/BII leakage:
NIST 188-01, Platform Services Division (PSD) **NIST 162-01, Commerce Business System, Core Financial System (CBS/CFS)** **NIST 640-01, Office of Reference Materials (ORM) System** **Pay.gov** **Technical controls are described in Section 8.2.**

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
Government Employees **Contractors**
Other:
Customers from the general public will have access to the NIST Storefront portal but will only be able to access their own account information.

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.

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.** **Yes, notice is provided by other means.**
The Privacy Act statement and/or privacy policy can be found at:
The general NIST Privacy Act Statement and/or privacy policy can be found at https://www.nist.gov/privacy-policy.
The reason why notice is/is not provided:
CRM: Notice is provided on the web form interface where inquiries are received by the public. It's recommended that notice is provided verbally when obtaining information in person. **E-Commerce: A Privacy Act Statement is found on customer registration profile pages:** https://shop.nist.gov/ccrz__CCSiteRegister?cartId=&portalUser=&store=&cclcl=en_US **The Privacy Act Statement is also presented in the shopping cart after selection of a product.**

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

Yes, individuals have an opportunity to decline to provide PII/BII.
The reason why individuals can/cannot decline to provide PII/BII:
CRM: Individuals have the opportunity to decline to provide PII/BII by not submitting a public inquiry or by not providing contact information. In doing so, they will not be able to obtain responses to inquiries with NIST and/or conduct business with NIST. **E-Commerce: A customer may decline to provide his/her PII, but then he/she will not be able to purchase NIST products and services. Products and services are targeted to scientific users, rather than the general public, and written acceptance of terms of use are required by NIST for the offered products and services.**

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.
The reason why individuals can/cannot consent to particular uses of their PII/BII:
CRM: Opportunity to consent to particular uses of PII/BII is provided on the web form interface where inquiries are received by the public. It's recommended that notice is provided verbally when obtaining the information in person. **E-Commerce: Customers have the ability to consent to particular uses of their individual profile information upon registration.**

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

Yes, individuals have an opportunity to review/update PII/BII pertaining to them.
The reason why individuals can/cannot review/update PII/BII:
CRM: Opportunity to review/update PII/BII is available through the person and/or system to whom they originally gave their information, or through the NIST external web portal at https://www.nist.gov/about-nist/contact-us. **E-Commerce: Customers have the ability to review/update their profile information at any time through the NIST storefront.**

<u>Section 8</u>: 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.
Access to the PII/BII is restricted to authorized personnel only.
Access to the PII/BII is being monitored, tracked, or recorded.

The information is secured in accordance with the Federal Information Security Modernization Act (FISMA) requirements.

The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.

NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 5 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).

A security assessment report has been reviewed for the supporting information system and it has been determined that there are no additional privacy risks.

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.

Reason why access to the PII/BII is being monitored, tracked, or recorded:

Access controls are in place as role-based permission are used.

The information is secured in accordance with FISMA requirements.

Is this a new system? No
Below is the date of the most recent Assessment and Authorization (A&A).
04/30/2021

Other administrative and technological controls for the system:

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

Unauthorized use of the system is restricted by user authentication, account management processes, and segregation of privileged user accounts and devices. Access logs are also kept and reviewed for anomalies.

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. Access to the administrative interface is limited to hardware using a NIST IP address, combined with user authentication (NIST-issued credentials).

All system connectivity is via TCP/IP across the NIST Network Infrastructure (SSP 181-04). The NIST Network Infrastructure system provides all services for physical cabling, network frame synchronization/flow control/error checking, routing, switching, and DNS.

Remote connections to NIST internal resources (i.e. telecommuting, travel, etc.) are made via SSL Remote Access services managed as part of the NIST Network Security system (SSP 181-01).

<u>Section 9</u>: Privacy Act

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

Yes, the PII/BII is 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.”

Yes, this system is covered by an existing system of records notice (SORN).
SORN name, number, and link:
CRM & E-Commerce [DEPT-2, Accounts Receivable 68 FR 35849](#) **– June 17, 2003** [DEPT-23, Information Collected Electronically in Connection with Department of Commerce Activities, Events, and Programs 78 FR 42038](#) **– July 15, 2013**
SORN submission date to the Department:

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.)*

Yes, there is an approved record control schedule.
Name of the record control schedule:
GRS 5.1/020 **Non-recordkeeping copies of electronic records** GRS 5.2/020 **Intermediary Records** GRS 6.5\010 **Public customer service operations records** GRS 6.5\020 **Customer/client records** **Note that information inputted into the CRM component from other information systems is referential and thus defers to the originating source of input to control the records.**
The stage in which the project is in developing and submitting a records control schedule:
Yes, retention is monitored for compliance to the schedule.
Reason why retention is not monitored for compliance to the schedule:

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

Disposal
Shredding **Deleting**
Other disposal method of the PII/BII:

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.

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

Factors that were used to determine the above PII confidentiality impact levels	Explanation
Identifiability **Quantity of PII** **Context of Use** **Obligation to Protect Confidentiality** **Access to and Location of PII**	**Identifiability The data types that are collected and maintained can be used to identify specific individuals.** **Quantity of PII: The quantity of the PII that is collected and maintained pertains to members of the public.** **The volume of data transmitted that may include other personally identifiable information is unknown.** **Context of Use: Customers providing information to obtain a product or service.** **Obligation to Protect Confidentiality: The organization is legally obligated to protect the PII within the applications.** **Access to and Location of PII: The data is stored in the cloud.**

<u>Section 12</u>: 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.)

The threat of unauthorized access and/or misuse exists but is reduced by effective security controls, internal user training and requiring internal users to sign relevant rules of behavior agreements.

Threats could arise from having multiple storefronts and subsequently multiple systems to transact E-Commerce. NIST centralized its E- Commerce systems into a single system to ensure consistency with management, administration, and technical controls.

A risk exists with authorized users entering inaccurate information into the CRM component. This risk is mitigated through internal user training. A risk also exists with the general public entering incorrect information into the E-Commerce solution. This risk is mitigated by allowing the general public to redress their information. In addition, the input field parameters have been limited in size to mitigate excessive input by the customer. **The use of NIST 162-01 CBS/CFS and Pay.gov services eliminates the need to process and store user's information in the BOO system, reducing risk associated with user's financial information.**

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

No, the conduct of this PIA does not result in required business process changes.
Explanation

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

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