Template Version Number: 01-2021

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

Privacy Threshold Analysis
for the
138-01 Business Operations Office (BOO) System

U.S. Department of Commerce Privacy Threshold Analysis

National Institute of Standards and Technology (NIST)

Unique Project Identifier: 138-01

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 from 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 and its purpose: *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).

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 purpose that the system is designed to serve
e) The way the system operates to achieve the purpose
f) A general description of the type of information collected, maintained, use, or disseminated by the system
g) Identify individuals who have access to information on the system
h) How information in the system is retrieved by the user
i) How information is transmitted to and from 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 purpose that the system is designed to serve
The mission of the NIST Business Operations Office (BOO) is to provide NIST with the service environment, processes, and partnerships needed for NIST to be a world leader in measurement science, standards, and technology. BOO fulfills this mission by partnering with service providers, customers, and NIST's external partners to develop and deliver products and services using project management, process engineering, relationship management, and customer engagement.

e. The way the system operates to achieve the purpose
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 support. 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, services or any related inquires. 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 calibration 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).

f. A general description of the type of information collected, maintained, use, or disseminated by the system
CRM - All data is Non-sensitive customer email and contact information.

E-Commerce – General personal data (GPD) and work-related data (WRD) to support the purchase of products and services from NIST. Public purchases may be from an individual or an organization.

g. Identify individuals who have access to information on the system
CRM - Salesforce admin with role-based permissions have access to the data.

E-Commerce – Public customers with accounts and system administrators have access to the system.

h. 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 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 that 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.

i. 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).

Questionnaire:

1. Status of the Information System

1a. What is the status of this information system?

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)
Other changes that create new privacy risks:

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

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.

Activities
Other activities which may raise privacy concerns:

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.)."

4. Personally Identifiable Information (PII)

4a. Does the IT system collect, maintain, or disseminate sensitive personally identifiable information (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."

The IT system collects, maintains, or disseminates sensitive PII about:

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?

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.

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

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.

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.

Is a PIA Required?	**Yes**

CERTIFICATION

__X__ The criteria implied by one or more of the questions above **apply** to the 138-01 Business Operations Office (BOO) System 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 138-01 Business Operations Office (BOO) System and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Information System Security Officer or System Owner Name: Schlatter, Katie Office: 01/4006B Phone: 303-497-4330 Email: katie.schlatter@nist.gov Signature: KATIE SCHLATTER Digitally signed by KATIE SCHLATTER Date: 2022.05.31 10:17:57 -06'00' Date signed: _____	**Chief Information Security Officer** Name: Heiserman, Blair Office: 225/A155 Phone: 301-975-3667 Email: nist-itso@nist.gov Signature: Digitally signed by BLAIR HEISERMAN Date: 2022.05.31 11:51:21 -04'00' Date signed: _____
Co-Authorizing Official Name: Vanek, Anita Office: 101/A1124 Phone: 301-975-3744 Email: anita.vanek@nist.gov Signature: ANITA VANEK Digitally signed by ANITA VANEK Date: 2022.06.27 10:29:01 -04'00' Date signed: _____	**Authorizing Official** Name: Sastry, Chandan Office: 225/B222 Phone: 301-975-6500 Email: chandan.sastry@nist.gov Signature: CHANDAN SASTRY Digitally signed by CHANDAN SASTRY Date: 2022.05.31 12:30:59 -04'00' Date signed: _____
Privacy Act Officer Name: Fletcher, Catherine Office: 101/A523 Phone: 301-975-4054 Email: catherine.fletcher@nist.gov Signature: CATHERINE FLETCHER Digitally signed by CATHERINE FLETCHER Date: 2022.05.27 13:23:03 -04'00' Date signed: _____	**Chief Privacy Officer** Name: Barrett, Claire Office: 225/B226 Phone: 301-975-2852 Email: claire.barrett@nist.gov Signature: CLAIRE BARRETT Digitally signed by CLAIRE BARRETT Date: 2022.05.31 21:43:54 -04'00' Date signed: _____