Version Number: 01-2015

U.S. Department of Commerce
National Institute of Standards and Technology

Privacy Impact Assessment
for the
Business Logistics System (162-03)
Customer Relationship Management (CRM) Component

Reviewed by: Delwin Brockett, 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 D. Purvis

Digitally signed by Catrina D. Purvis
DN: cn=Catrina D. Purvis, o=Office of the Secretary, Office of Privacy and Open Government, ou=US Department of Commerce, email=cpurvis@doc.gov, c=US
Date: 2017.02.06 17:17:34 -05'00'

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/Business Logistics System

Unique Project Identifier: 162-03

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 Business Logistics System encompasses several enterprise components (e.g., applications) used to support business transactions for NIST. This Privacy Impact Assessment (PIA) specifically addresses Customer Relationship Management (CRM), which is one component of this system. The purpose of CRM is to enable NIST to manage interactions and relationships with their customers, and review how NIST provides products, services, and support. This is made possible by aggregating customer data from other authorized NIST systems into the CRM. To ensure appropriate review and validation of data, CRM is being implemented in phases. This PIA is applicable to phase II.

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

The following are examples of transactions using the CRM component which may contain Personally Identifiable Information (PII) or Business Identifiable Information (BII):

1. Manage the status and award of Cooperative Research and Development Agreement (CRADA);
2. Manage business identifiable information related to partners and stakeholders of Manufacturing Centers;
3. Identify people who have been invited to, registered for, and/or attended public conferences hosted by NIST;
4. Manage non-sensitive customer email and contact information copied by NIST staff from Microsoft Office 365, entered via a public facing web form, or entered via a mobile application.

(c) any information sharing conducted by the system

The CRM will share information with other internal NIST business units.

(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 section 12 of the Stevenson-Wydler Technology Innovation Act of 1980, as amended, 15 U.S.C. 3710a.

(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.
__X_ 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	X	g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	X
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify): Aggregation of data from other NIST systems.					

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		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:					

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	X	d. Telephone Number	X	g. Salary	
b. Job Title	X	e. Email Address	X	h. Work History	
c. Work Address	X	f. Business Associates	X		
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):					

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	X	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): *public facing portal					

Government Sources					
Within the Bureau	X	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):			

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): A mobile application to scan customer provided business cards, and a web portal for inputting customer data directly into CRM.			

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			
To determine eligibility		For administering human resources programs	
For administrative matters		To promote information sharing initiatives	
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).

The 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, thus allowing NIST to better understand customer needs. For example, CRM allows NIST to proactively manage public inquiries by ensuring a timely response, or acquire insight into the types of speakers or attendees at conferences and other events. 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.

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			
Federal agencies			
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 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.

	The CRM receives input from components of the following NIST information systems: 1. 100-02, Associate Directors' Offices System 2. 480-01, MEP Enterprise Information System (MEIS)
	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

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		Government Employees	X
Contractors	X		
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: The general NIST Privacy Act statement and/or privacy policy can be found at https://www.nist.gov/privacy-policy	
X	Yes, notice is provided by other means.	Specify how: Notice is provided on the web form interface where inquiries are received by the public. Notice is also provided verbally when obtaining information in person.
	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 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 transact business with NIST.
	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: Opportunity to consent to particular uses of PII/BII is provided on the web form interface where inquiries are received by the public. Notice is also provided verbally when obtaining information in person.
	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: 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.
	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: Access logs are kept and reviewed for anomalies.
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): FedRAMP Moderate Authorization to Operate, 05/23/2014. NIST Authorization to Operate, 01/2017. ☐ 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).
X	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
X	Contracts with customers establish ownership rights over data including PII/BII.
X	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 CRM system is hosted by a cloud vendor that has a FedRAMP issued Authority to Operate. Data is stored at the vendor's storage sites, which are within the continental United States. Data-at-rest encryption is employed using CRM's FIPS validated encryption (AES 128) on selected data fields. Access logs are kept and reviewed for any anomalies.

There is a public facing web interface which permits anyone to submit information into CRM. The interface uses the Secure Socket Layer (SSL) protocol, and thus encrypts data flowing between the web interface and the backend CRM. Interface fields restrict data input. All other access to CRM requires NIST-issued credentials because access is restricted by user authentication.

Remote users access CRM by first connecting to the NIST network through a Virtual Private Network (VPN). Mobile device users may utilize a CRM mobile application which allows a direct front-end into the CRM, using the TLS 1.2 protocol, encrypting end-to-end communication.

To mitigate risk associated with mobile devices, only Government-furnished equipment (NIST-owned) may be used with the mobile application. Attachments can only be viewed, not downloaded locally to the device. NIST mobile devices require full device encryption and mobile device management (MDM). MDM uses full device FIPS validated encryption on Android devices, and FIPS validated encryption or encryption that is in process for FIPS validation for iOS devices. MDM also enforces inactivity periods, password management, etc.

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."

X	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name and number *(list all that apply)*: SORN Commerce/DEPT-23 Information Collected Electronically in Connection with Department of Commerce Activities, Events, and Programs
X	Yes, a SORN has been submitted to the Department for approval on June 2016.
	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.)*

X	There is an approved record control schedule. Provide the name of the record control schedule: GRS 4.2 Information Access and Protection Records

	GRS 4.3 Input Records, Output Records, and Electronic Copies **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.
	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		Overwriting	X
Degaussing		Deleting	X
Other (specify):			

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.)*

X	Identifiability	Provide explanation: The data types that are collected and maintained can be used to identify specific individuals and businesses, and their NIST interests.
X	Quantity of PII	Provide explanation: The quantity of the PII that is collected and maintained pertains to federal employees, federal contractors, foreign nationals, members of the public, or partners and stakeholders.
X	Data Field Sensitivity	Provide explanation: Each field within data inputs is reviewed for sensitivity.
X	Context of Use	Provide explanation: The CRM enables NIST to manage interactions and relationships with their customers, and review how NIST provides products, services, and support.
X	Obligation to Protect Confidentiality	Provide explanation: The organization is legally obligated to

		protect PII, and BII specific to CRADA awards.
X	Access to and Location of PII	Provide explanation: The data for the CRM component is stored by a cloud vendor.
X	Other: Aggregation	Provide explanation: The aggregation of the various data inputs is considered.

Section 12: Analysis

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

X	Yes, the conduct of this PIA results in required business process changes. Explanation: Existing disparate information is uploaded into a single repository, and the direct collection of additional information directly into the system is enabled. System life cycle addressed to incorporate verification of privacy controls at various developmental stages.
	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.

X	Yes, the conduct of this PIA results in required technology changes. Explanation: New component application.
	No, the conduct of this PIA does not result in any required technology changes.