Version Number: 01-2017

U.S. Department of Commerce
Minority Business Development Agency

Privacy Threshold Analysis for the MBDA Salesforce Customer Relationship Management (MSFCRM)
FY 2019

U.S. Department of Commerce Privacy Threshold Analysis

MBDA Salesforce Customer Relationship Management System

Unique Project Identifier: [Number]

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 general description of the information system in a way that a non-technical person can understand.*

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

The MBDA Salesforce CRM System (MSCRM) is a major application that contains specific information regarding each of MBDA's minority business enterprise clients. The CRM system supports the MBDA grant program.

b) System location

The system is a cloud based FedRAMP accredited Software as a Service (SAAS) system.

c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)

The CRM system is a stand-alone system.

d) The purpose that the system is designed to serve

The CRM system is a major application that supports the MBDA grant program. The system is a cloud based FedRAMP accredited Software as a Service (SAAS) system. It is used to support the performance of the MBDA Business Centers by receiving input from the business centers and project operators. MBDA Staff reviews the input data and uses the information provided to determine the performance of the grant award. Data is input by the business centers at remote locations and submitted into the system. The MBDA staff can access the data in real time.

Using the Customer Relationship Management System, MBDA collects and stores PII information on business center operators, and sensitive BII pertaining to MBDA clients, and partners. The information includes industry codes, financial and business history information, and other business plan information that if disclosed improperly, could create competitive harm to businesses. Information regarding minority businesses (clients) is also collected from clients and other non-client sources (e.g., third party websites, brokers). The MBDA business centers collect client information and data to analyze the clients' financial, contract, and market potential in order to provide technical business services. The data is used by the MBDA headquarters program office to monitor the performance of the grantees, to make policy decisions, and to provide specialized services to the business centers. MBDA uses the potentially sensitive financial, transactional and industry BII and race/ethnicity information collected from minority business enterprises to determine eligibility for participation as clients of the MBDA Business Center program.

e) The way the system operates to achieve the purpose

The MBDA Headquarters and MBDA business center staff and grantees retrieve information from the system using centralized and consistent processes for internal user provisioning with user profiles, permission sets and strong authentication mechanisms. The E-Mail/SMS-based identity confirmation feature enables users to log in from unrecognized devices to receive a one-time 5-digit PIN delivered via SMS to a registered phone number before being granted access to the system. MBDA Headquarters and Business Center staff can access the data in the system on a real-time basis.

A typical transaction includes the input of specific client information and data in the system in various fields by the MBDA Business Centers. MBDA Staff reviews the input data and uses the information provided to determine the performance of the grant award. Data is input by the business centers at remote locations and submitted into the system. The MBDA staff can access the data in real time.

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

The MBDA Salesforce CRM System (MSCRM) contains specific information regarding each of MBDA's minority business enterprise clients, general customers, and strategic partners. MBDA uses Business Identifiable Information (BII) and race/ethnicity information collected from minority business enterprises to determine eligibility for participation as clients of the MBDA Business Center program and to other MBDA Projects. See Executive Order 11625, section 6(a) and 15 CFR section and 15 CFR section 1400.1(b). MBDA also captures client service information and related outcomes (i.e. contract and financial awards received) to measure performance and validate success of the programs.

Using the Customer Relationship Management System (CRM), MBDA collects and stores PII on Business Center and Project Operators, and BII on MBDA clients and partners. The information includes NAICs, business capability, business history information, contract and finance capacity/capability and other business information relevant to matching/referring/ supporting business development for MBEs, if disclosed improperly, could create competitive disadvantage to

the businesses or partners.

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

The MBDA headquarters program office staff and MBDA National Director, and staff have access to information on the system. The MBDA Business Centers are federal grantees who have access to system to input information to allow the MBDA business centers collect staff to monitor the performance of the grantees, to make policy decisions, and to provide specialized services to the business centers.

h) How information in the system is retrieved by the user

The E-Mail/SMS-based identity confirmation feature enables users to log in from unrecognized devices to receive a one-time 5-digit PIN delivered via SMS to a registered phone number before being granted access to the system.

i) How information is transmitted to and from the system

Information is transmitted to and from the system by end-to-end TLS/ HTTPS (v1.2 or higher) cryptographic protocols utilized to encrypt network data transmissions. Secure routing and traffic flow policies ensure that traffic is encrypted entering MSCRM until the load balancer decrypts the traffic. The load balancers decrypting the traffic are FIPS 140-2 compliant and are located inside of the Salesforce Government Cloud isolation boundary. Network devices enforce traffic flow policies in the Salesforce Government Cloud.

Questionnaire:

1. 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	
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):					

__X__ 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.*

_____ 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 01-2015 or later). *Skip questions and complete certification.*

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.

__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 about: *(Check all that apply.)*

__x__ Companies
__x__ Other business entities

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

4. Personally Identifiable Information

4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?

As per OMB 07-16, Footnote 1: "The term 'personally identifiable information' refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc... alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc..."

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

____ DOC employees

____ Contractors working on behalf of DOC
__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 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.

4c. 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, and/or 4c are "Yes," a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the approved PIA must be a part of the IT system's Assessment and Authorization Package.

CERTIFICATION

__X__ I certify the criteria implied by one or more of the questions above **apply** to the **OS-066 MBDA Salesforce Cloud System** and as a consequence of this applicability, I will perform and document a PIA for this IT system.

_____ I certify the criteria implied by the questions above **do not apply** to the **OS-066 MBDA Salesforce Cloud System** and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of Information System Security Officer (ISSO) or System Owner (SO):
Efrain Gonzalez

Signature of ISSO or SO: _____ Date: 4/18/19

Name of Information Technology Security Officer (ITSO): Jun Kim

Signature of ITSO: JUN KIM Digitally signed by JUN KIM DN: c=US, o=U.S. Government, ou=Department of Commerce, ou=Office of the Secretary, cn=JUN KIM, 0.9.2342.19200300.100.1.1=13001001483988 Date: 2019.04.25 17:30:33 -04'00' Date: _____

Name of Authorizing Official (AO): Terryne F. Murphy

Signature of AO: TERRYNE MURPHY Digitally signed by TERRYNE MURPHY DN: c=US, o=U.S. Government, ou=Department of Commerce, ou=Office of the Secretary, cn=TERRYNE MURPHY, 0.9.2342.19200300.100.1.1=13001000472785 Date: 2019.05.19 17:01:49 -04'00' Date: _____

Name of Bureau Chief Privacy Officer (BCPO): Josephine Arnold

Signature of BCPO: JOSEPHINE ARNOLD Digitally signed by JOSEPHINE ARNOLD Date: 2019.04.12 17:14:59 -04'00' Date: _____