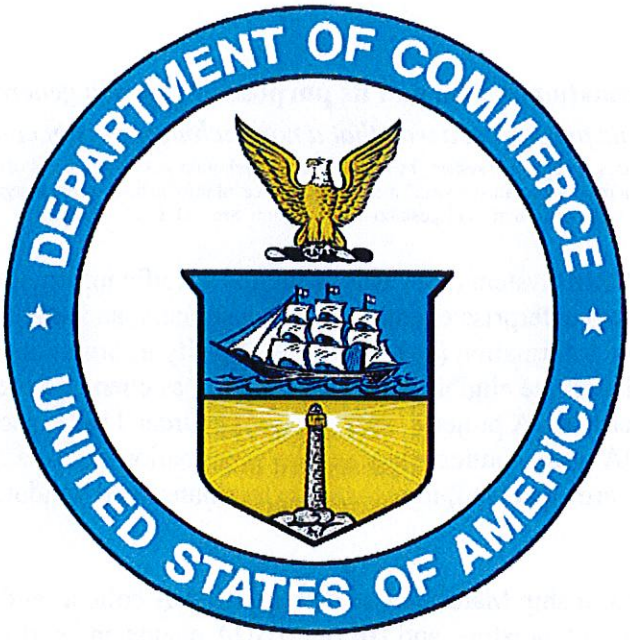
Version Number: 01-2015

U.S. Department of Commerce
Minority Business Development Agency



Privacy Threshold Analysis
for the
MBDA Salesforce Customer Relationship Management (MSFCRM)
FY 2017

U.S. Department of Commerce Privacy Threshold Analysis

MBDA 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 and its purpose 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).

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 from minority business enterprises to determine eligibility for participation as clients of the MBDA Business Center program and other MBDA projects. See Executive Order 11625, section 6(a) and 15 CFR § 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, 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.

Questionnaire:

1. What is the status of this information system?

____ This is a new information system. *Continue to answer questions and complete certification.*

__X__ ☐ 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	x
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):					

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

_x___ Yes. *Please describe the activities which may raise privacy concerns.*

The information in the system is shared in real time with MBDA business development specialists and staff in the Washington, DC office and may be shared with other federal agencies for specific purposes related to research. Race and ethnicity data will be collected regarding the specific business owners. Any disclosure of information regarding a business, financial or other sensitive confidential information, could impact the competitive position of the business in the marketplace.

____ 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 (System Owner)

Signature of ISSO or SO: _____ Date: 2/28/17

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

Signature of ITSO: _____ Date: 2/28/2017

Name of Authorizing Official (AO): **Rod Turk**

Signature of AO: _____ Date: 3/3/17

Name of Bureau Chief Privacy Officer (BCPO): Joey Hutcherson, OS Privacy Officer:
Josephine Arnold

Signature of BCPO: _____ Date: 3/6/17