Template Version Number: 01-2020

U.S. Department of Commerce
Minority Business Development Agency

Privacy Impact Assessment
for the
MBDA Salesforce Customer RelationshipManagement (MSFCRM)

JOSEPHINE ARNOLD Digitally signed by JOSEPHINE ARNOLD Date: 2021.08.26 13:54:29 -04'00'

Reviewed by: _____, 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

Jennifer Goode 09/17/2021

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer Date

U.S. Department of Commerce Privacy Impact Assessment
Minority Business Development Agency
MBDA Salesforce Customer Relationship System

Unique Project Identifier: OS-66

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) 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 staff and grants 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 way the system operates to achieve the purpose(s) identified in Section 4
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 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 and specialty programs (MBC/MSP) and to provide technical business services to clients.

(e) How information in the system is retrieved by the user
The MBDA Headquarters and MBDA business center and specialty program 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.

(f) How information is transmitted to and from the system

A typical transaction includes the input of specific client information and data in the system in various fields by the MBDA Business Centers and Specialty Program. 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. No changes have been made to the system from FYI 8, everything remains the same.

(g) Any information sharing conducted by the system

The information collected in the CRM by MBDA Business Centers and Specialty Programs (grantees) is shared in real time and on a continuous basis with the MBDA Headquarters (grantor) for the purpose of monitoring business center performance. The information may be shared with other federal agencies for specific purposes related to research on a case by case basis. There is no pre-determined sharing with other federal agencies, however, the MBDA may share information in an aggregated format with the U.S. Census Bureau.

(h) The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information

MBDA collects, maintains, uses and disseminates the information pursuant to delegated authority from the Secretary of Commerce to execute programs and activities under Executive Order 11625(codified at 15 CFR section 1400). Pursuant to EO 11625, MBDA has the authority to provide financial assistance to public and private organizations so that they may render technical and management assistance to minority business enterprises and defray all or part of the costs of pilot or demonstration projects conducted by public or private agencies or organizations which are designed to overcome the special problems of minority business enterprises. MBDA competes, awards, and manages federal financial assistance awards (MBDA Business Center awards) to external organizations that provide direct technical business assistance to minority businesses on behalf of the Agency. The MBDA business centers collect the client BII and data to provide technical business services. The data is used by the MBDA Headquarters program office to monitor the performance of grantees, to make policy decisions, and to provide specialized services to the business centers.

(i) The Federal Information Processing Standards (FIPS) 199 security impact category for the system

Moderate impact (access control, audit, and accountability).

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.
_____ 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		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.
____ 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 01-2017).
____ 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 01-2019 or later).

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*		f. Driver's License		j. Financial Account	
b. Taxpayer ID		g. Passport		k. Financial Transaction	
c. Employer ID		h. Alien Registration		l. Vehicle Identifier	
d. Employee ID		i. Credit Card		m. Medical Record	
e. File/Case ID	X				
n. Other identifying numbers (specify):					
*Explanation for the business need to collect, maintain, or disseminate the Social Security number, including truncated form:					

General Personal Data (GPD)					
a. Name	X	h. Date of Birth		o. Financial Information	
b. Maiden Name		i. Place of Birth		p. Medical Information	
c. Alias		j. Home Address	X	q. Military Service	
d. Gender	X	k. Telephone Number	X	r. Criminal Record	
e. Age		l. Email Address	X	s. Physical Characteristics	
f. Race/Ethnicity	X	m. Education		t. Mother's Maiden Name	
g. Citizenship		n. Religion			
u. Other general personal data (specify):					

Work-Related Data (WRD)					
a. Occupation		e. Work Email Address	X	i. Business Associates	X
b. Job Title	X	f. Salary		j. Proprietary or Business Information	X
c. Work Address	X	g. Work History		k. Procurement/contracting records	
d. Work Telephone Number	X	h. Employment Performance Ratings or other Performance Information			
l. Other work-related data (specify):					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		f. Scars, Marks, Tattoos		k. Signatures	
b. Palm Prints		g. Hair Color		l. Vascular Scans	
c. Voice/Audio Recording		h. Eye Color		m. DNA Sample or Profile	
d. Video Recording		i. Height		n. Retina/Iris Scans	
e. Photographs		j. Weight		o. Dental Profile	
p. 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	f. Queries Run	X	f. Contents of Files	X
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	
Telephone	X	Email	X		
Other (specify):					

Government Sources					
Within the Bureau	X	Other DOC Bureaus	X	Other Federal Agencies	X
State, Local, Tribal	X	Foreign			
Other (specify):					

Non-government Sources					
Public Organizations	X	Private Sector	X	Commercial Data Brokers	
Third Party Website or Application			X		
Other (specify):					

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

The accuracy of the information is ensured by an internal verification process conducted by the MBDA Headquarters program staff. Headquarters program staff reviews the information input into the system by the Business Centers and verifies the accuracy of the documents and data.

2.4 Is the information covered by the Paperwork Reduction Act?

X	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection. **0640-0002**
	No, the information is not covered by the Paperwork Reduction Act.

2.5 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):			

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			
For a Computer Matching Program		For administering human resources programs	
For administrative matters	X	To promote information sharing initiatives	X
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)	X
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).

This refers to members of the public, specifically businesses. MBDA, primarily through the MBDA Business Center program participants, collects the following data fields (see section 2.1) for use in: (a) providing technical and business development services to minority businesses; (b) for organizations and businesses that serve as MBDA business centers; and (c) for MBDA staff to track and monitor performance related to MBDA programs.

1) For administrative matters: the metrics recorded into the system are used by the grant officials of MBDA and NOAA to determine whether the grant recipients are meeting the performance goals required by the Federal Funding Opportunity Announcement, the 0MB regulations, and the MBDA program requirements.
2) To promote information sharing initiatives: as an ancillary use, the information collected may be shared with other federal agencies as a result of the Administration's data initiatives.
3) To improve Federal services online: the information recorded in the system will provide MBDA with information to determine the type of information and services to be provided on the public website at

www.mbda.gov.

4) For employee or customer satisfaction: data collected by the system, including the customer/client survey responses, is used by MBDA to gauge the adequacy of service provided by the MBDA headquarters staff and the MBDA business centers.
5) For web measurement and customization technologies: all data collected by the system will be analyzed to assess the technical and practical effectiveness of the CRM system as a tool for the MBDA services provided and to determine whether additional customization is required to maximize the use of the system for the program.

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.)

The security for the MSCRM application cover multiple security controls with regards to protecting the confidentiality, integrity, and availability of MBDA sponsored information systems and the information processed, stored, and transmitted by those systems. The security areas include: access control; awareness and training; audit and accountability; certification, accreditation, and security assessments; configuration management; contingency planning; identification and authentication; incident response; maintenance; media protection; physical and environmental protection; planning; personnel security; risk assessment; systems and services acquisition; system and communications protection; and system and information integrity. The MSCRM application team has implemented the required security controls based on the tailoring guidance of NIST Special Publication 800-53 Rev 4 and the Department's policies and procedures.

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	X		
Federal agencies	X	X	
State, local, tribal gov't agencies			
Public			
Private sector			
Foreign governments			
Foreign entities			
Other (specify):			X

	The PII/BII in the system will not be shared.

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

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

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. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage:
X	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

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			
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: https://www.mbda.gov/page/privacy-policy .	
X	Yes, notice is provided by other means.	Specify how: Electronic copy provided to Centers. See Appendix A.
	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: By declining to provide the information requested by the MBDA Business Center during the initial interview.
	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: On the client intake and transaction verification forms at the input level with the MBDA Business Center or MBDA Business Development Specialist.
	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: Upon request from the Business Center representative and as a Privacy Act request to FOIA@mbda.gov.
	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 to PII/BII is recorded as a selection box and monitored and tracked through continuous services provided by the ISSO. Only authorized personnel can access the system.
X	The information is secured in accordance with the Federal Information Security Modernization Act (FISMA) requirements. Provide date of most recent Assessment and Authorization (A&A): 3/18/2021 ☐ 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 (POA&M).

X	A security assessment report has been reviewed for the information system and it has been determined that there are no additional privacy risks.
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 DOC 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. *(Include data encryption in transit and/or at rest, if applicable).*

Data security is achieved through the combination of security controls offered by the Salesforce Government Cloud network infrastructure, database management systems and resource management. To ensure the consistent implementation of security controls across the various layers of infrastructure and services, Salesforce has implemented an organization- wide security program consistent with commercial (e.g., ISO 27001, SSAE16, PCI) and U.S. Government (e.g., FIPS 200 and NIST 800-53 Rev. 4., FedRAMP moderate) requirements and practices including but not limited to the following:

ACCESS CONTROL
• Centralized and consistent processes for internal user provisioning
• Assignment of access and separation of functions based on job responsibilities
• User profiles, permission sets and respective roles define their level of accessibility
• Limiting the number of concurrent sessions allowed per user
• Implementing automated system notification and deactivation of user accounts due to inactivity (30, 60 & 90 days)

IDENTIFICATION AND AUTHENTICATION
• Strong authentication mechanism for system users and processes
• The E-Mail/SMS-based identity confirmation: This feature enables users logging 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

AUDIT AND ACCOUNTABILITY
• Logging and auditing of system logs
• Login history: a six-month history of all login attempts to the org, including user name, IP address, success/failure, and time and date is available upon demand.
• Audit trail logs: a 180-day history of setup changes made by the system administrator is also available upon demand and can be used to troubleshoot and audit administrative activities.
• Record Modification Fields Tracking: All objects include fields to store the name of the user who created the record and who last modified the record. This provides some basic auditing information.
• Field History Tracking

NETWORK SECURITY
• Connections to the system are served over TLS (HTTPS) with a 2048-bit Public Key. The Services use International/Global Step Up certificates, with AES 256-bit encryption by default.

DATABASE SECURITY
• The database is hardened according to industry and vendor guidelines. User passwords for the system are hashed via a salted SHA 256 algorithm before being stored in the database.
PASSWORD POLICIES
• Password complexity and expiration settings within MBDA SFCRM instance is configured to comply with DOC internal policies. The available password settings include:
  - Password expiration timers
  - Prevent re-use of previous passwords
  - Password complexity restrictions
  - Invalid lockout attempts
  - Lockout timers

Section 9: Privacy Act

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

_X__ Yes, the PII/BII is searchable by a personal identifier.

___ No, the PII/BII is not 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."

X	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name, number, and link. *(list all that apply)*: **DEPT-IO, Executive Correspondence Files; DEPT-23, Information Collected Electronically in Connection with Department of Commerce Activities, Events and Programs; DEPT-25 Access Control and Identity Management System**
	Yes, a SORN has been submitted to the Department for approval on (date).
	No, this system is not a system of records and a SORN is not applicable.

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: **NARA General Records Schedule 3**
	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	
Other (specify):			

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.
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 level. *(Check all that apply.)*

X	Identifiability	Provide explanation: Each business is identified by several indicators in the records.
	Quantity of PII	Provide explanation:
X	Data Field Sensitivity	Provide explanation: Data fields regarding financial, annual revenues and contract financial information are sensitive.
	Context of Use	Provide explanation:
X	Obligation to Protect Confidentiality	Provide explanation: If applicable to BII, the Trade Secrets Act (**18** USC§ 1836, as amended bv PL 114-153 (2016)).
	Access to and Location of PII	Provide explanation:
	Other:	Provide explanation:

Section 12: 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.)

There are no potential threats to personal privacy existing based on the information collected or sources. Threats related to the collection of BII concerning company financial information, requests for funding or merger/acquisition potential are mitigated by the lack of fields in those sensitive areas. This information is not recorded into the system but may be provided to the Business Center for use in

servicing the client.

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

	Yes, the conduct of this PIA results in required business process changes. Explanation:
X	No, the conduct of this PIA does not result in any required business process changes.

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

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

APPENDIX A

Privacy Policy

Thank you for visiting an Minority Business Development Agency (MBDA) web site. MBDA's mission is to achieve entrepreneurial parity for MBEs by actively promoting their ability to grow and compete in the global economy. In support of its activities, MBDA is occasionally required to collect business or personal information from our customers. We do not collect this type of information without the voluntary consent of the site visitor.

The main purpose of this policy is to inform our visitors that you have rights under the Privacy Act, that all business or personal information provided to MBDA is on a voluntary basis, and that information provided will be protected to the extent permitted by the Privacy Act of 1974 and the Freedom of Information Act of 1966. At each location where information is collected, we make every effort to explain explicitly how the information you provide will be used, and we allow you to determine if you consent to provide such information. Voluntarily submitting information constitutes your consent for MBDA to use the information for the purpose stated and indicates to us you are aware of MBDA's Privacy Policy provisions. For more information on the Freedom of Information Act and your rights under the Privacy Act please visit the Federal Citizen Information Center site at https://www.usa.gov/.

Our sites do not use "persistent cookies" or any persistent tracking technologies that can identify a specific visitor, or information about that visitor, over multiple visits. However, some MBDA websites do use "session cookies" that identify the visitor for the duration of a browsing session. Session cookies are deleted from our Web servers when your session ends.

MBDA does collect certain non-personal information to help us better service our site visitors. Information collected includes for example: the IP (Internet Protocol) address from which you accessed our site; the IP address of the website from which you linked to us; the name of your domain; the type of browser and operating system you are using; the date and time our site is accessed; and the

pages visited. This information does not identify you personally.

Information Collected from E-Mail, Forms and through Site Registration:

Information you submit may be viewed by various people within the MBDA, its funded projects and other Federal agencies actively involved in supporting minority entrepreneurs.. If you register on one of our web sites to obtain a benefit, or use any of our services, you may submit personally identifiable information, such as name, title, name/size of company, or address. Certain MBDA services are reserved for U.S. firms and we may use the registration information to contact you for verification purposes before allowing access to the requested service. Information collected from the public on our websites has been authorized by The Office of Management and Budget (OMB) (http://www.whitehouse.gov/omb/) as required under the Paperwork Reduction Act.

Security, Intrusion, and Detection:

Unauthorized attempts to upload or change information, or otherwise cause damage to our websites, are strictly prohibited and may be punishable under applicable Federal law. Data traffic is monitored in order to identify unauthorized activities and to help ensure that MBDA Web services remain available to our users.

Search Engine Indexing Policy:

This site uses a tool which collects your requests for pages and passes elements of them to search engines to assist them in indexing this site. MBDA controls the configuration of the tool and are responsible for any information sent to the search engines.

Links to Other Web Sites:

Our websites contain links to other federal agencies and private organizations. Websites of those organizations may contain links to outside organizations. This linking does not constitute an endorsement by MBDA. These links are provided for user convenience only.

The appearance of hyperlinks to other sites does not constitute endorsement by the Minority Business Development Agency of these web sites or the information, products or services contained therein.

Regarding non-MBDA web sites, we do not exercise any editorial control over the information you may find at these locations. These links are provided consistent with MBDA's stated purpose as shown on our web site.

We recommend that you review the website's information collection policy or terms and conditions to fully understand what information is collected and/or provided.

For more information, please review the Department of Commerce Privacy Policy Statement at https://www.commerce.gov/privacy-policy.