Version Number: 01-2019

U.S. Department of Commerce- Office of Chief Information Office (OCIO)

&

Economic Development Administration (EDA)

Privacy Impact Assessment
for the
EDA Salesforce – Customer Relationship Management

Reviewed by: Jeffrey Roberson, 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 03/30/2021

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

U.S. Department of Commerce Privacy Impact Assessment
EDA Salesforce – Customer Relationship Management

Unique Project Identifier: OS-066 and Sub-System OS-066C

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 EDA SF-CRM is a major application system supporting all EDA grant programs.

(b) System location.

It is in Salesforce Government Cloud environment. Salesforce uses infrastructure provided by Amazon Web Services, Inc. ("AWS") to host Customer Data submitted to Salesforce Maps.

Salesforce Government Cloud is both Software as a Service (SaaS) and Platform as a Service (PaaS).

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

EDA-SF-CRM will be interconnected with DOC Microsoft Outlook Exchange Server. Data is transferred to and from these systems. However, no PII or BII data is transmitted.

(d) The way the system operates to achieve the purpose(s) identified in Section 4.

The EDA Salesforce Customer Relationship Management (EDA-SF-CRM) system aims to increase the ability of EDA staff and management to provide support and assistance to its stakeholders, including its existing and potential grantees. To achieve EDA's mission, staff and management must communicate with existing stakeholders and create new connections. EDA-SF-CRM aims to enable the storage, tracking, and analysis of the organizations with which EDA works, the individuals at those organizations with whom EDA has relationships, and the projects, referrals, and partnerships—potential and realized—that EDA may fund or in which EDA may participate. By achieving this goal, EDA-SF-CRM will support EDA in its efforts to increase the speed at which it deploys assistance to communities, the effectiveness of EDA assistance, and the quality and consistency of its relationships through staffing changes and across geographically dispersed offices and staff.

Salesforce will also specifically provide EDA Community Portals that will have the capability to manage two EDA grant programs: Revolving Loan Fund (RLF) and Trade Adjustment Assistance for Firms (TAAF). Grants requested under these programs are processed in EDA's grant system named Operations Planning and Control System (OPCS). After the grant is approved and the grant recipient receives the award/funds, the grant is currently tracked outside the OPCS system consistent with program requirements. Salesforce provides the following capabilities for these programs:

- RLF - EDA issues funds to the non-profit RLF Recipients (formally known as grantee). The RLF Recipients disburse money in the form of loans from the fund to small businesses that cannot otherwise borrow capital in the open market. These loans are provided at an interest rate that is at or below current market rate. The RLF Recipients must report on the loans they issue and the total capital base of the fund.

  Salesforce will enable EDA RLF Administrators (internal users) to track /monitor the RLF program and ensure that the RLF Recipient (external non-federal users) are complying with their grant award terms and RLF Plan, including distributions of the grant funds to small businesses as loans. In addition, Salesforce will provide all RLF Recipients the capability to submit their reports to EDA consistent with program requirements. RLF Administrators use these reports collect and analyze relevant information pertaining to the loan portfolio and grant status.

- TAAF- The mission of the TAAF program is to help import impacted U.S. manufacturing, production, and service firms develop and implement projects to regain global competitiveness, expand markets, strengthen operations, increase profitability, thereby increasing U.S. jobs.

  The TAAF program funds a national network of 11 Trade Adjustment Assistance Centers (TAACs), some of which are university-affiliated and others of which are independent non-profit organizations. The TAACs are the EDA grantees. The TAAF program is administered and managed by EDA's Trade Adjustment Assistance for Firms Division.

  Prospective firms work with the TAACs in a public-private collaborative framework to apply for certification of eligibility for TAAF assistance and then prepare and implement strategies to guide their economic recovery (Proposals or Adjustment Proposals). The costs are shared using certain criteria, with up to 50 percent Federal Share (via the grants awarded to TAACs) and 50 percent contribution from the benefiting firm.

  Petitions and Adjustment Proposals (Aps) are prepared and submitted by the TAACs. Firms do not apply directly to EDA for certification. EDA does not interface with Firms at all in this process. Firms will not be Salesforce Users. *Note: APs process is not implemented in Salesforce.*

Salesforce provides access for the 11 TAACs (external non-federal users) nationwide to create and update petition submissions and allow TAAF agents (EDA internal users) to review the submissions and monitor the program.

(e) How information in the system is retrieved by the user?

EDA-SF-CRM records, which consist of *organizations*, *contacts*, and *projects (grant information)*, may be retrieved by identifying information associated with each respective record. Project details are derived primarily from EDA grant application documentation and is principally public information. The remaining information contained in the system consists solely of contact information and program information. Contact information identifies individuals and organizations in their professional capacities. However, in some cases, individuals may provide general personal data even though it is strongly encouraged to provide their work-related information.

Program data provides information to help track/monitor the grant programs and performance information. The grantee (grant recipient) provides most of this information. The data may be retrieved by identifying information associated with each respective record.

The above data may be accessed only by EDA authorized users (internal and external). EDA personnel may share the data manually on a case-by-case basis with other DOC and Federal staff. However, it is *not shared outside the programs.*

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

EDA staff, particularly EDA Economic Development Representatives (EDRs), collect professional contact information for individuals and organizations manually through various means, including through in-person exchanges at meetings, conferences, and events; through oral discussions conducted via telephone or web conference; through email exchanges; and through grant proposal and application documentation submitted via mail, facsimile, and grant applications forms downloaded from Grants.gov. Professional contact information will be manually entered into EDA-SF-CRM by EDA users or transferred into EDA-SF-CRM directly through electronic means, such as DOC email systems. Contact information and potential or actual/required project (grant) information are entered into EDA-SF-CRM. The system provides manual file upload capability for various types of data when there are numerous records required to be added to the application. The data types that can be manually uploaded are various contact information, applicant grant information, EDA funding sources and appropriation, and Census Tract. EDA users also obtain data from public websites such as StatsAmerica.org, Census.gov and FEMA.gov. For example, the data collected for Census Tract and FEMA disasters.

The RLF and TAAC external users will manually input the required information so EDA employees may track/monitor these programs.

(g) Any information sharing conducted by the system?

EDA-SF-CRM records, which consist of *organizations, contacts,* and *projects (grant information),* may be retrieved by identifying information associated with each respective record. Most information contained in the system for EDA staff consists solely of contact information that identifies individuals and organizations, some administrative grant tracking information (e.g., grant tracking number, award amount, date of award, etc.), and program information (e.g., APs, petitions). These data may be accessed only by EDA internal authorized users and may be shared manually on a case-by-case basis with other DOC and Federal staff.

The RLF and TAAC external users may retrieve their program data by identifying information associated with each respective record. These data may be accessed only by EDA internal and external authorized users. It may be shared manually by EDA internal users on a case-by-case basis with other DOC and Federal staff. However, it is *not shared outside the programs.*

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

EDA may collect and maintain personally identifiable Information (PII) and business identifiable Information (BII) within EDA-SF-CRM pursuant to its authorizing statutes, which includes the Public Works and Economic Development Act of 1965, as amended (42 U.S.C. § 3121 *et seq.*), Chapters 3 and 5 of the Trade Act of 1974, as amended (19 U.S.C. 2341 *et seq.* and 19 U.S.C. 2391 *et seq.*), and Sections 25-28 of the Stevenson-Wydler Technology Innovation Act of 1980, as amended 15 U.S.C. § 3720-3723).

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

The Security Categorization Level is Moderate.

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

__X___ 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):					

___ 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).

____ 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 01-2017 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	X	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					
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		q. Military Service	
d. Gender		k. Telephone Number	X	r. Criminal Record	
e. Age		l. Email Address	X	s. Physical Characteristics	
f. Race/Ethnicity		m. Education		t. Mother's Maiden Name	

g. Citizenship		n. Religion			
u. Other general personal data (specify):					

Work-Related Data (WRD)					
a. Occupation	X	e. Work Email Address	X	i. Business Associates	X
b. Job Title	X	f. Salary		j. Proprietary or Business Information	
c. Work Address	X	g. Work History			
d. Work Telephone Number	X	h. Employment Performance Ratings or other Performance Information			
k. 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		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	
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.

Users will be sent messages to ensure EDA validates their data. There are several data sets that can be manually uploaded when there is a large number of records or if a file is received from anther data source. This upload feature will minimize manual data entry mistakes.

2.4 Is the information covered by the Paperwork Reduction Act?

	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection.
X	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	
For web measurement and customization technologies (single-session)		For web measurement and customization technologies (multi-session)	
Other (specify): To determine applicant eligibility and track program level data.			

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).

EDA staff, particularly EDA Economic Development Representatives (EDRs), collect professional contact information for individuals and organizations through various means, including through in-person exchanges at meetings, conferences, and events; through oral discussions conducted via telephone or web conference; through email exchanges; and through grant proposal and application documentation submitted via mail, facsimile, or Internet portal (e.g., grants.gov). Professional contact information may be manually entered into EDA-SF-CRM by EDA users or may be transferred into EDA-SF-CRM directly through electronic means, such as through interfaces to the FEMA website. While only professional contact information and potential or actual project information is entered into EDA-SF-CRM, in some cases, individuals may provide general personal data even though it is strongly encouraged to provide their work-related information.

Information collected is from Federal agencies, members of state, local, and tribal governments, and institutions of higher education, nonprofits, and other organizations that are eligible for EDA grants or with which EDA otherwise collaborates or engages. This would also include businesses that applied to an EDA RLF grantee for a loan or to a TAAC for adjustment assistance under TAAF.

The system will provide manual file upload capability for about 16 different data files. The manual file upload is used when there are numerous records that need to be uploaded from other data sources.

The information may be shared manually on a case-by-case basis with other DOC bureaus and other Federal agencies to facilitate coordinated responses to grant inquiries that cross DOC bureaus or other agency programs. However, program data is only shared within 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.)

There is potential for insider threat.

Users, system administrators, and Salesforce personnel that are responsible for handling sensitive data are trained.

The data is disposed of by shredding documents and deleting or overwriting records. Only the System Administrator has the capability to delete records.

Authorized Salesforce personnel use level data to provision and provide the Salesforce server support. Access is controlled by authentication. User access within the application is logged and monitored.

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		
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.

	Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage: The name of the system that is connected to Salesforce is DOC HCHB NOC/Outlook. The following are the technical controls in place: • When data is transferred from HCHB Outlook e-mail to Salesforce using a user or group e-mail account, the account is configured to interact using the correct Salesforce URL. • The Outlook system must be configured to grant an application access in Outlook Office 365. The user must have the Outlook Add-in on their computer to have this configured. DOC Exchange Technician has to add and configure the software. • Salesforce Inbox requires permission via an OAuth flow tool to access a user's Outlook Office365 email inbox. Salesforce requires Admin approval for a user to connect to an Office365 account in Salesforce Inbox. This does not apply to the Community Portals for TAAF and RLF. The portals do not provide this capability.
	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): Two sets of external users can access information submitted by the external user and generated by EDA that is specific to that user for RLF Operators (grant recipients), TAACs (grant recipients), and potential grant recipients.			

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.

	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: _____.	
	Yes, notice is provided by other means.	Specify how:
	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: The individual may decline to provide the data to EDA staff. In addition, the individual may decline to provide the data on the Grants.gov forms, by not completing the fields. However, the individual/organization (applicant) must provide information on the form for the grant request to be processed. This applies to all EDA grants including for the RLF and TAAF grants. In order to determine eligibility of a business to receive a loan under the RLF program and assistance under the TAAC program, the applicant must provide information to determine eligibility. They may decline to provide such information, but their respective eligibility could consequently not be determined, and they would not receive a loan or assistance.
	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: When individuals or organizations provide contact information to EDA staff, they effectively give consent for it to be used to discuss potential EDA assistance or other collaborations. In addition, when an individual/organization (applicant) or entity completes a grant application, he/she effectively gives consent for it to be used to determine whether the organization qualifies for a grant. There are no other uses for this information than the application itself. This applies to all EDA grants including for the RLF and TAAF programs.

		RLF Loan Recipient - When an entity voluntarily completes a loan application, the individual/organization gives consent for the information to be used to determine whether he/she qualifies for a loan. There are no other uses for this information. TAAF – When an organization voluntarily submits a petition, the organization gives consent for the information to be used to determine qualification. There are no other uses for this information.
	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: For the CRM, individuals and organizations may contact EDA to update the information. For RLF program, the information is accessed and updated via the RLF program reporting process which is semi-annual. The RLF Recipients submit updates for the semi-annual report and can change the information at that time. For the TAAF program, the information is accessed and updated by TAACs and EDA TAAF Division. The TAACs can update information submitted in the petitions.
	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: EDA-SR-CRM tracks use account login information.
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): _____ ☒ 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.
	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).*

Access controls for authorized users are implemented on production systems through the use of unique usernames and passwords. NIST Special Publication (SP) 800-53 rev 4 access controls are enforced for access the application. User accounts are obtained through system administrators, who act as application account managers. Upon initial login, users are prompted to change their system-assigned initial password.

Users or processes acting on behalf of users are uniquely identified through user accounts. Password authentication is in place and required for all user accounts, applications, and system access. This level of authentication meets NIST SP 800-63 guidance. Passwords must adhere to current DOC guidelines (minimum length, aging, history, combination of character types, etc.) before access is granted.

In addition to using User ID and password, the Salesforce Native Two Factor Authentication (Salesforce Authenticator App) is used. Single Click Approve/Deny from the mobile device. A code is sent to the user mobile device. The user must enter the code to finish the login process.

The above also applies to the Community Portals (external users).

Access logs are kept and reviewed for any anomalies.

PII (contact data) and BII data are encrypted at rest via Salesforce Platform Encryption and in transit via TLS/SSL.

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)*: COMMERCE/DEPT-10: Executive Correspondence Files COMMERCE/DEPT-23: Information Collected Electronically in Connection with Department of Commerce Activities, Events, and Programs.
	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: EDA uses the General Record Retention schedule. The following General Records Schedules are used for `EDA-SF-CRM`: • General Records Schedule used 1.2: Grant and Cooperative Agreement Records DAA Disposition Authority: DAA-GRS2013-00080001 • General Records Schedule 6.5: Public Customer Service Records; DAA-GRS-

	2017-00020002
	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	X	Overwriting	X
Degaussing		Deleting	X
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 levels. *(Check all that apply.)*

	Identifiability	Provide explanation:
X	Quantity of PII	Provide explanation: EDA-SR-CRM applications contains different types of PII data fields identified in Section 2.1.
X	Data Field Sensitivity	Provide explanation: The EDA-SR-CRM applications contain sensitive BII.
	Context of Use	Provide explanation:

X	Obligation to Protect Confidentiality	Provide explanation: The data contains PII and BII data that confidentiality must be protected.
	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 known potential threats to privacy in the context of this system. The PII and BII data are collected to process grants, determine the eligibility of the grantee, and to report program information (for RLF and TAAF). In addition, the PII data is collected to conduct outreach to EDA customers and stakeholders.

12.2 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: A privacy notice will be added when individuals sign up for the events or on the actual sign-in sheet.
	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.