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

&

Economic Development Administration

E·D·A

U.S. ECONOMIC DEVELOPMENT ADMINISTRATION

Privacy Threshold Analysis
for the
EDA Salesforce - Customer Relationship Management

U.S. Department of Commerce Privacy Threshold Analysis

EDA Salesforce Customer Relationship Management (EDA SF-CRM)

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

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 (in a way that a non-technical person can understand) of the information system that addresses the following elements:*

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 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 are transmitted.

d) The purpose that the system is designed to serve.

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. In addition, 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).

e) The way the system operates to achieve the purpose

The EDA-SF-CRM system will increase the ability of EDA staff and management to provide support and assistance to its stakeholders, including its existing and potential grantees. It will allow EDA staff and management to 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.

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

EDA-SF-CRM records, which consist of *organizations*, *contacts*, and *projects (grant information*). 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).

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

The type of individuals that have access to the system are EDA internal authorized users (e.g. federal, contractors, interns, detailee) and grant recipients. 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.

h) 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.*

i) 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.

Questionnaire:

1. What is the status of this information system?

_X___ 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):					

____ 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). *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 01-2017 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. *(Check all that apply.)*

Activities			
Audio recordings		Building entry readers	
Video surveillance		Electronic purchase transactions	
Other (specify):			

__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.

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

4. Personally, Identifiable Information (PII)

4a. Does the IT system collect, maintain, or disseminate PII?
As per OMB 17-12: "The term PII refers to information that can be used to distinguish or trace an individual's identity either alone or when combined with other information that is linked or linkable to a specific individual."

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

__X__ DOC employees
____ National Institute of Standards and Technology Associates
__X__ Contractors working on behalf of DOC
____ Other Federal Government personnel
__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 Social Security numbers (SSNs), including truncated form?

____ Yes, the IT system collects, maintains, or disseminates SSNs, including truncated form.

Provide an explanation for the business need requiring the collection of SSNs, including truncated form.

Provide the legal authority which permits the collection of SSNs, including truncated form.

__X__ No, the IT system does not collect, maintain, or disseminate SSNs, including truncated form.

4c. 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.

4d. 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.

__N__ 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, 4c, and/or 4d 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 **EDA SF-CRM** 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 [IT SYSTEM NAME] 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): Sandranette Moses, Information System Owner

Signature of ISSO or SO: SANDRANETTE MOSES Digitally signed by SANDRANETTE MOSES Date: 2020.05.06 09:00:28 -04'00' Date: 5/06/2020

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: 2020.06.18 13:36:27 -04'00' Date: _____

Name of Privacy Act Officer (PAO): Jeffrey Roberson

Signature of PAO: JEFFREY ROBERSON Digitally signed by JEFFREY ROBERSON Date: 2020.05.06 10:31:25 -04'00' Date: _____

Name of Authorizing Official (AO): Lawrence Anderson

Signature of AO: LAWRENCE ANDERSON Digitally signed by LAWRENCE ANDERSON Date: 2020.06.23 13:23:38 -04'00' Date: _____

Name of Bureau Chief Privacy Officer (BCPO): Jeffrey Roberson

Signature of BCPO: JEFFREY ROBERSON Digitally signed by JEFFREY ROBERSON Date: 2020.05.06 10:32:06 -04'00' Date: _____