PRIVACY IMPACT ASSESSMENT FOR CUSTOMER RELATIONSHIP MANAGEMENT (CRM) SYSTEM (MICROSOFT DYNAMICS 365)

July 28, 2022

Record of Approval

Document Approval		
USAC PRIVACY POC		
Laurence H Schecker		**Senior Advisor - Associate General Counsel and Privacy Officer**
Signature DocuSigned by: Laurence Schecker 2AFA2492613041F...	**Date** 7/28/2022	
Accepted by:		
Elliot S. Tarloff		**FCC Senior Agency Official for Privacy**
Signature DocuSigned by: Elliot S. Tarloff 9000F2444A314E2...	**Date** 7/28/2022	

Version History

Date	Description	Authors
7/28/2022	Initial PIA	Laurence Schecker, Mitchell Calhoun, Max Mansur, Nima Mehri, Steven Strandberg

TABLE OF CONTENTS

Application Cloud

1.1. Introduction

Section 208 of the E-Government Act of 2002[1] requires agencies to conduct a **Privacy Impact Assessment (PIA)** whenever they procure or develop an information technology system that will collect, maintain, or disseminate information about individual people. The PIA must document how the system will use information it collects about individuals and, unless it contains classified or sensitive information, it must be made available to the public. The PIA was intended to be a tool for agencies to protect personal information throughout a technology system's life cycle. The Office of Management and Budget (OMB) has commented: "*In general, PIAs are required to be performed and updated as necessary where a system change creates new privacy risks.*"[2]

The Federal Communications Commission (FCC) is subject to the requirements of the E-Government Act and is committed to identifying and addressing privacy risks whenever it develops or makes changes to its information systems. The questions below explore important privacy issues identified in the Act and in later guidance by OMB and the National Institute of Standards and Technology (NIST). A longer discussion of the FCC's PIA policies can be found in Chapter 9 of the FCC's Privacy Act Manual (FCC Inst. 1113.1).

System owners, in collaboration with the Information System Security Officers (ISSOs) should complete the **Initial Privacy Assessment (IPA)** prior to filling out the PIA. The Universal Service Administrative Company (USAC) Privacy Officer, in consultation with the FCC Senior Agency Official for Privacy (SAOP), uses the IPA to determine whether a system will collect the kind of information that would make it subject to the requirements of Section 208 of the E-Government Act, including a PIA. A PIA should not be completed until an IPA is completed and the SAOP makes a determination that a PIA is necessary.

If you have any questions, please contact the USAC Privacy Officer at privacy@USAC.org or the FCC Privacy Team at privacy@FCC.gov.

[1] 44 U.S.C. § 3501 note.

[2] OMB Memorandum No. M-03-22 (Sep. 26, 2003), https://www.whitehouse.gov/wp-content/uploads/2017/11/203-M-03-22-OMB-Guidance-for-Implementing-the-Privacy-Provisions-of-the-E-Government-Act-of-2002-1.pdf.

1.2. Authority To Operate (ATO) Boundary Overview

For each IT system that resides within the ATO Boundary, please use the table below to provide the system name, a brief description of the what the system does, whether it contains Personally Identifiable Information (PII) and a brief description of the PII (if applicable), the applicable System of Records Notice, the legal authorities to collect and maintain the PII, and whether the PII is shared with other systems (internal or external).

INFORMATION ABOUT THE SYSTEM
NAME OF THE SYSTEM APPLICATION Customer Relationship Management (CRM)
DOES THE SYSTEM CONTAIN PII? Yes
PLEASE PROVIDE A BRIEF DESCRIPTION OF THE PII (IF APPLICABLE) By design, the system will collect full name, phone number, email address from each stakeholder (including both program participants and those individuals supporting the program participants such as consortiums, consultants, and service providers, depending on the program) that initiaties contact with the system. The system also will collectbusiness PII from CRM system internal users (the USAC employees and contractors that are authorized to use CRM) such as full name and business email address. CRM system internal users may need to collect additional information (such as physical business address or partial banking information) to verify a stakeholder's identity. Additional PII may be submitted, even though unsolicited, and then ingested into the CRM system. This happens when, stakeholders provide additional PII to CRM system internal users acting as customer service agents. Such PII elements may include date of birth, home address, place of birth, sex, email address, work address, Social Security Number (SSN) or other taxpayer ID number, facsimile number, mother's maiden name, official certfiicates (birth, death, etc.), relevant legal documents (divorce decrees, etc.), limited financial information (account numbers), employment status, military/veteran status, and a driver's license or other state-issued ID.
IN WHAT SYSTEM OF RECORDS NOTICE (SORN) IS THE INFORMATION CONTAINED (IF APPLICABLE)? Business Contacts and Certifications System of Records Notice (SORN), FCC-2, and the Lifeline SORN, FCC/WCB-1 , both posted on the FCC's website at https://www.fcc.gov/managing-director/privacy-transparency/privacy-act-information
WHAT ARE THE LEGAL AUTHORITIES FOR THE COLLECTION OF THIS PII? 47 U.S.C. § 254; 47 C.F.R. Part 54.

DOES THE COMMISSION KEEP AN ACCURATE ACCOUNTING OF DISCLOSURES FROM THE SYSTEM AS REQUIRED BY SUBSECTION (c) OF THE PRIVACY ACT? Yes.
DOES THIS SYSTEM SHARE THE PII WITH OTHER SYSTEMS? No.

A. Is this a new ATO Boundary or an existing ATO Boundary?

☒ New Boundary

☐ Existing Boundary

B. If the ATO Boundary is/will consist of cloud-based computing system(s),[3] please check the box that best describes the service USAC receives/will receive from the cloud computing provider:

☒ USAC uses provider-supported application/s on the provider's cloud network (Software as a Service or SaaS)

☐ USAC has deployed application/s on the provider's cloud network and the provider supports the applications (Platform as a Service (PaaS)) Appian Cloud

☐ USAC has deployed its own application/s on the cloud network and controls how these application/s are configured and operate (Infrastructure as a Service or IaaS)

C. If the IT systems in the ATO Boundary are in the cloud, are the they FedRAMP certified?

☒ Yes, all the IT systems are FedRAMP certified

☐ No, none, or only some, of the IT systems are FedRAMP certified

[3] *See* NIST, *The NIST Definition of Cloud Computing*, Special Pub. No. 800-145 (Sep. 2011), https://csrc.nist.gov/publications/detail/sp/800-145/final.

1.3. Collection of Data

A. Please explain why it is necessary to collect PII to carry out the purpose of each of the system(s) that maintain PII within this Boundary.

CRM by design collects limited PII from stakeholders in order to identify their records within other existing USF or appropriated fund systems so that CRM system internal users can review stakeholder files and resolve their complaint or assistance requests. As explained above, stakeholders may potentially provide other unsolicited PII.

B. For each system within this Boundary, will this PII be collected from individuals themselves, or from third-parties? If collected from individuals themselves, link to the Privacy Act Notice[4] for each system that is included with the online or paper form the system(s) use(s) to collect the PII.

The PII in the CRM system will be collected from individuals, from representatives of individuals, and from individuals acting in a business capacity (i.e., individuals who are working as employees or representatives of organizational stakeholders) for entities who participate in Universal Service Fund (USF) or appropriated programs administered by USAC for the FCC. The system will also include limited business PII from CRM system internal users.

The CRM system does not use paper forms. It receives emails and sometimes written communications and can incorporate requests for assistance that are made to USAC via telephone.The privacy notice that will be contained in replies to emails or hard copy inquiries is attached as an Addeendum to this document. That same privacy notice will be utilized when USAC implements a portal for consumers to access the CRM.

C. What steps is USAC taking to limit the collection of PII to only that which is necessary?

When information is received via email, CRM system internal users will retain only the PII elements in CRM that are necessary to complete the support request; they will remove unnecessary PII from any CRM case files and all PII from outgoing communications. Even after after CRM system internal users remove unneeded PII from the CRM case file and from any responsive communications, stakeholder PII may remain in the Exchange email account from which the CRM system draws the case information. When PII is received via

[4] A Privacy Act Notice must inform individuals about (1) the authority to solicit information, (2) the principal purpose(s) for collecting the information, (3) the routine uses for disclosing the information, and (4) whether providing the information is mandatory or voluntary.

telephone or written form, CRM system internal users will upload only necessary PII elements to the CRM system to complete the request.

D. What steps will USAC take to make sure this PII is accurate, complete, and up-to-date?

The CRM system collects limited PII by design. Stakeholders are generally aware that without providing accurate information, CRM system internal users will not be able to accurately respond to their inquiries. Stakeholders are therefore responsible for ensuring the information provided is accurate, complete, and up-to-date. Stakeholders may voluntarily provide documents with additional PII if they feel it would be relevant to their inquiry. They are also responsible for the accuracy of any such PII provided. As necessary, the USAC customer service and support-focussed personnel will update PII in the system that is required to support service requests, when provided by USF and appropriated program participants.

1.4. Use of the Data

A. Please explain the data flow, including whether the PII will be ingested from, or shared with, another system.

The CRM system will ingest PII from a variety of systems and sources. Email inquiries are received by a USAC Microsoft Exchange email account connected to the CRM system. CRM will copy the contents of emails received from that account and create a case file in CRM for the submitted assistance request. When stakeholders contact USAC via telephone, stakeholder PII necessary to respond will be entered into the CRM. No PII contained in CRM will be electronically shared with another system, although CRM system internal users may use the PII to access information about individuals in other systems.

B. Will the information be shared with third-parties as part of the operations of the information system (e.g., through an application programming interface or "API")?

No.

C. How long will the PII be retained and how will it be disposed of?

All data in CRM are retained as required by the FCC's requirements and adopted in the USAC data retention schedule. Data from USF programs contained in the CRM system are retained in accordance with schedules mandated by the National Archives and Records Administration (NARA), and require retention for 10 years (or longer if there is a business need to retain the records). NARA has not adopted a schedule for ACP records, and until a schedule is adopted the ACP records will be retained indefinitely. USAC adheres to National Institute of Standards and Technology (NIST) guidelines for the destruction of records.

1.5. Data Security and Privacy

A. What are the system's ratings for confidentiality, integrity, and availability?

Confidentiality	**__High**	**_X__Moderate**	**___Low**
Integrity	**__High**	**_X__Moderate**	**___Low**
Availability	**__High**	**_X__Moderate**	**___Low**

B. Discuss the physical, administrative, and technical controls in place to protect the data in the system.

The CRM system has been implemented with security and privacy controls in compliance with (and assessed and authorized under) NIST SP 800-53 Revision 5 controls as documented in the System Security Plan (SSP) for CRM. The control sources include, both as shared and fully provided controls, the FedRAMP authorized controls as described in the Microsoft Azure Dynamics 365 SSP, the Enterprise Common Controls (ECC) as described in the ECC SSP, and the General System Support (GSS) as described in the GSS SSP. System specific or system shared/hybrid controls are specified in the CRM SSP. All controls have been assessed by an independent third party, and a provisional ATO has been issued so that the system can transition from development to production (in phases) including final steps to compy with controls identified as findings in the assessment and to migrate data to production prior to issuing an unqualified ATO.

C. Does the system inherit privacy controls from an external provider? If an Interconnection Security Agreement (ISA) , Memorandum of Understanding (MOU) , or similar document is in place, please summarize the privacy applicable portions of the document.

The CRM system inherits, fully or partially, as defined in the SSP, privacy controls from the Cloud Service Provider (CSP) Microsoft Azure for Dynamics 365 Software-as-a-Service FedRAMP authorized offering. There is no ISA or MOU required for FedRAMP authorized CSP offerings.

1.6. Access to the Information

A. Which types of users will have access to the PII in this information system?

Approved CRM system internal users will have access to the information in the CRM system on a need-to-know basis and for authorized purposes only. The CRM system may generate reports accessible only to limited USAC staff, contractors, and FCC staff on a need-to-know basis and for authorized purposes only. Reports may also be generated and provided pursuant to inquiries received under applicable law.

B. Does this system leverage Enterprise Common Controls (ECC)?

Yes. As discussed in section 1.5 B, CRM inherits controls from GSS and ECC.

ADDENDUM

Privacy Act Statement

This Privacy Act Statement explains how we are going to use the personal information in this system.

The Privacy Act is a law that requires the Federal Communications Commission (FCC) and the Universal Service Administrative Company (USAC), as the FCC's program administrator, to explain why we are asking individuals for personal information, and what we are going to do with this information after we collect it.

Authority: 47 U.S.C. § 254; 47 CFR Part 54.

Purpose: The USAC Customer Relationship Management (CRM) system is a comprehensive customer service complaint and assistance request management system that allows Universal Service Fund (USF), Emergency Connectivity Fund (ECF), and Affordable Connectivity Program (ACP) stakeholders (including both program participants and those individuals supporting the program participants such as consortiums, consultants, and service providers, depending on the program) to submit complaints and requests for assistance from USAC via email and telephone calls to a managed call center. The USAC CRM system collects personal information to identify and verify users, communicate with them about their issues, and track issues to resolution. .

Routine Uses: We may share the personal information you enter into this form with other parties for specific purposes, such as:

- With USAC employees and contractors who operate the CRM system;
- With service providers who participate in the Universal Service Fund and appropriated fund programs in order to help resolve consumer complaints and inquiries;
- With appropriate agencies, entities, and persons when the FCC suspects or has confirmed that there has been a breach of information; and
- With law enforcement and other officials investigating potential violations of FCC rules.

A complete listing of the ways we may share your information is published in the Business Contacts and Certifications System of Records Notice (SORN), FCC-2, and the Lifeline SORN, FCC/WCB-1 , both posted on the FCC's website at https://www.fcc.gov/managing-director/privacy-transparency/privacy-act-information.

Disclosure: You are not required to provide the identifying information we are requesting, but if you do not, we will not be able to provide the assistance you seek.