UNITED STATES

FEDERAL COMMUNICATIONS COMMISSION

PRIVACY IMPACT ASSESSMENT (PIA) FOR THE DISASTER INFORMATION REPORTING SYSTEM (DIRS) BOUNDARY[1]

July 2023

OFFICE OF GENERAL COUNSEL

Washington DC, 20554

Next Review Cycle: July, 2024

Record of Approval

Document Approval		
Drafter Name: Alexander Egorov		**Bureau/Office: PSHBA**
SAOP Approval		
Printed Name: Elliot S. Tarloff		**Senior Agency Official for Privacy**
Signature: ELLIOT TARLOFF Digitally signed by ELLIOT TARLOFF Date: 2023.07.11 11:31:26 -04'00'	**Date**	

Record of Approval

Date	Description	Author
05/11/2023	Validation of information – System Owner	Michael Caiafa
06/15/2023	Validation of completeness – IT Compliance Lead	Liem Nguyen

Revision History

Date	Description	Name
10/12/2022	Original Document Created	ISSO – Alexander Egorov
01/10/2023	Minor Updates	ISSO
05/09/2023	Final Edits	ISSO
7/11/2023	Formatting revisions	Senior Agency Official for Privacy (SAOP) – Elliot S. Tarloff

DIRS System Boundary

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 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 the Office of Management and Budget (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 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, including a PIA. A PIA should not be completed until an IPA is completed and the SAOP makes a determination.

If you have any questions, please contact the 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/sites/whitehouse.gov/files/omb/memoranda/2003/m03_22.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 The Disaster Information Reporting System (DIRS)
NAME OF BUREAU Public Safety and Homeland Security (PSHSB)
DOES THE SYSTEM CONTAIN PII? Yes. When establishing a CORES and DIRS account, a user's name, email address, and phone number are collected. After submitting this PII, a user may view the information by signing in using the DIRS credentials. DIRS administrators may obtain PII related to files by logging into DIRS. Administrators of DIRS conduct searches based on the names of individuals and the names and locations of carriers.
PLEASE PROVIDE A BRIEF DESCRIPTION OF THE PII (IF APPLICABLE) The DIRS gathers just the PII required to contact users, such as the full name, work phone number, and work email address of a user.
IN WHAT SYSTEM OF RECORDS (SORN) IS THE INFORMATION CONTAINED (IF APPPLICABLE)? Business Contacts and Certifications System of Records Notice,FCC-2
WHAT ARE THE LEGAL AUTHORITIES FOR THE COLLECTION OF THIS PII? 47 U.S.C. §§ 151, 154(i)-(j) & (o), 251(e)(3), 254, 301, 303(b), 303(g) & (r), 332, 403, and 1302.
DOES THE COMMISSION KEEP AN ACCURATE ACCOUNTING OF DISCLOSURES FROM THE SYSTEM AS REQUIRED BY SUBSECTION (c) OF THE PRIVACY ACT? Yes. The Privacy Team keeps an accurate accounting of disclosures of information.
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 the FCC receives/will receive from the cloud computing provider:

☐ The FCC uses provider-supported application/s on the provider's cloud network (Software as a Service or SaaS) [list applicable system(s)]

☐ The FCC has deployed application/s on the provider's cloud network and the provider supports the applications (Platform as a Service or PaaS) [list applicable system(s)]

☒ The FCC 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) [Amazon Web Services]

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

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

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.

The Federal Communications Commission (FCC) needs to gather the contact information of entities who make use of the DIRS so that it may communicate with entities about any data that may be questionable or erroneous.

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 Statement[4] for each system that is included with the online or paper form the system(s) use(s) to collect the PII.

For each system within this Boundary, the PII will be collected directly from the individuals themselves, rather than from third parties. The Privacy Act Statement pertaining to the collection of PII is readily accessible on the front page, located beneath

[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.

[4] A Privacy Act Statement 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.

the login section. To review the Privacy Act Statement for each system involved in the collection of PII, please follow the provided link: https://dirs-uat-internal.fcc.gov/

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

The DIRS application requests that respondents give just the personally identifiable information data elements that are required for the Commission or other entities to get in touch with them.

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

It is the responsibility of the DIRS users to ensure that the information they provide is correct, comprehensive, and up-to-date. If a user uploads erroneous information, he or she may correct the information or contact the DIRS staff to have the data corrected.

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. Are internal connections reflected in the Cyber Security Asset Management tool (CSAM)? Are Information Sharing Agreements (ISAs) in CSAM for external connections?

The DIRS ingests personally identifiable information directly from users using CORES and OKTA. While contact information is collected and used for communication purposes, there are other connections and sharing mechanisms in place. Connections between DIRS and CORES are reflected in CSAM.

Moreover, information can be provided from DIRS to participating state agencies, subject to certifications submitted by these agencies. Additionally, DIRS can share information with DIRS filers upon the filer's request and approval by PSHSB. Thus, while DIRS does not generally share personally identifiable data with other systems and organizations, there are specific instances and processes in place that allow for the sharing of such information under certain conditions.

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?

Information in the systems within this boundary is retained and destroyed in accordance with applicable FCC policies and procedures, as well as with the FCC records disposition schedule or General Records Schedules approved by the National Archives and Records Administration (NARA).

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 FCC protects its information resources with a dynamic set of security measures. Some of these measures (e.g., network firewalls, physical security) protect the entire FCC enterprise, while other measures (e.g., user access restrictions, encryption) are applied to specific information systems. Following the risk-based policy established in the Federal Information Modernization Act (FISMA), the FCC applies more security measures (also known as security "controls") to information systems that present higher operational risks. Consistent with this policy, the FCC applies specific security controls to systems that collect and process PII. A comprehensive list of the security and privacy controls the FCC may apply to its information systems can be found in National Institute of Standards and Technology (NIST) Special Publication No. 800-53, Revision 5 [NIST].

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.

Yes. Amazon Web Services East/West – FedRAMP

1.6 Access to the Information

A. Which FCC employees and contractors will have access to the PII in this information system?

DIRS Admin users only

B. Does this system leverage Enterprise Access Controls?

Yes, the URS utilizes Okta and CORES for authentication, login, and access.