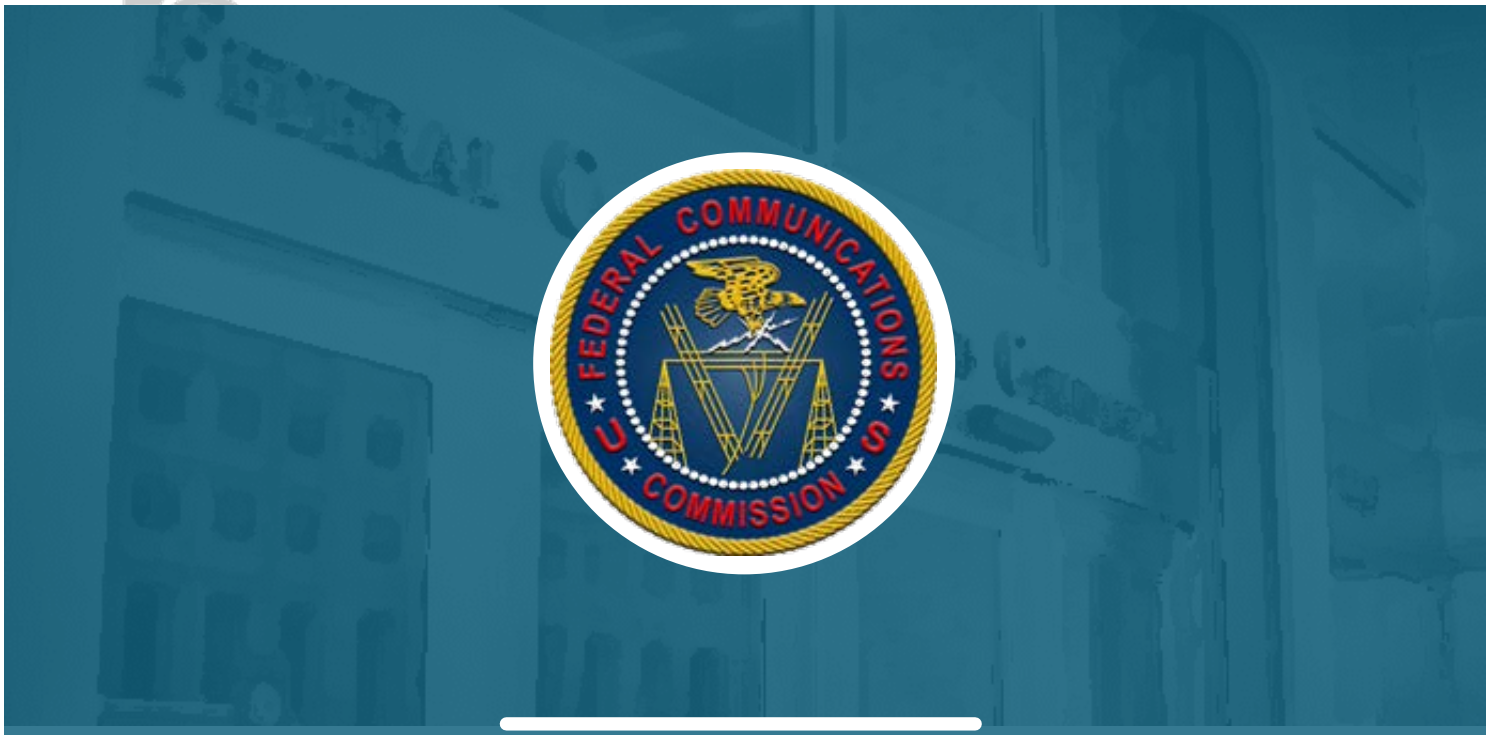

UNITED STATES

**FEDERAL COMMUNICATIONS COMMISSION**

# PRIVACY IMPACT ASSESSMENT FOR THE GENESIS SYSTEM BOUNDARY

**February 4, 2021**


**OFFICE OF THE GENERAL COUNSEL**

WASHINGTON, DC 20554

# Record of Approval

| Document Approval | | |
|---|---|---|
| **Privacy POC** | | |
| **Printed Name:** Bahareh Moradi | | |
| **Approval Structure** | | |
| **Printed Name:** Margaret Drake | | **Senior Agency Official for Privacy** |
| **Signature:**<br>Margaret E Drake<br>Digitally signed by Margaret E Drake<br>DN: cn=Margaret E Drake, o=Federal Communications Commission, ou=Privacy, email=margaret.drake@fcc.gov, c=US<br>Date: 2021.02.04 09:51:57 -05'00' | **Date**<br>2/4/21 | |

# Record of Approval

| Date | Description | Author |
|---|---|---|
| | | |
| | | |
| | | |
| | | |
| | | |

# Table of Contents



# List of Tables

# Genesis 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).

Please copy the table as necessary to complete the information for each system within the boundary.

| **INFORMATION ABOUT THE SYSTEM** |
|---|
| NAME OF THE SYSTEM<br><br>Genesis |
| DOES THE SYSTEM CONTAIN PII?<br><br>Yes |
| PLEASE PROVIDE A BRIEF DESCRIPTION OF THE PII (IF APPLICABLE)<br><br>Genesis is the Office of Managing Director, Financial Operations Center's (OMD-FO) integrated, financial IT system that records current financial planning, purchasing, accounts receivable, accounts payable, disbursements (including payroll) , and other financial and budget activities, including FCC employees' government credit card information. Genesis is structured so that financial transactions automatically update budget, financial planning, and general ledger data when processed. |
| IN WHAT SYSTEM OF RECORDS (SORN) IS THE INFORMATION CONTAINED (IF APPPLICABLE)?<br><br>FCC/OMD-25, Financial Operations Information System (FOIS) |
| WHAT ARE THE LEGAL AUTHORITIES FOR THE COLLECTION OF THIS PII?<br><br>44 U.S.C. 3101, 3102, and 3309; Debt Collection Act as amended by the Debt Collection Improvement Act of 1996; Federal Managers Financial Integrity Act of 1982; Accountability of Tax Dollars Act, P.L. 107-289; and other government-wide federal financial statutes addressing debt collection, budget control, financial controls, fraud, waste and abuse, and internal controls codified in Title 31 United States Code. |
| DOES THIS SYSTEM SHARE THE PII WITH OTHER SYSTEMS?<br><br>Yes. |

**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):

Genesis is comprised of the Momentum Commercial off-the-shelf (COTS) software. In 2019, Genesis was migrated to CGI's Azure Tenant Cloud.

**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

Genesis inherits controls from the FedRAMP Azure environment, Okta (for user authentication), and the FCC Common Controls.

## 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 FCC collects PII in this system in order to (1) process and track payments made and monies owed from or to individuals; (2) create tax records to be reported to federal,

[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.

state, and local tax authorities; (3) track auction loans and payment history; (4) track employee Government credit cards; and (5) track debts owed to the FCC.

**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.**

The PII within this boundary is not collected directly from individuals, rather it is ingested from other systems.

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

The FCC's Financial Operations ingests the least amount of PII necessary to process the financial transactions of individuals who conduct business with the Commission. The FCC's Financial Operations will continue monitoring the data and business needs to ingest the least amount of PII necessary in the future.

**What steps will the FCC take to make sure this PII is accurate, complete, and up-to-date?**
Genesis ingests PII from other systems and relies on those systems to ensure that the PII collected is accurate and complete. Genesis ensures that the PII is current by ingesting records from these systems daily.

## 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?**

Genesis ingests PII from CORES, the Invoice Processing Platform (IPP), and the USDA. Information in the Genesis System is shared within the FCC, including EBATS, Servive Now, and ULS. Genesis also shares financial information with the U.S. Treasury, and the

[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.

U.S. Department of Agriculture (USDA), USAC, the National Archive and Records Administration (NARA), and TRS (Telecommunications Relay Services).

Some of the connections are reflected in CSAM, specifically EBATS, ServiceNow, and ULS. The connections with USDA, CORES, NARA, and TRS are not reflected in CSAM. The ISAs are not stored in CSAM.

**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")?**

Genesis shares information under the various Congressionally-mandated Federal financial statutes and regulations that cover debt collection, budget control, financial controls, fraud, waste and abuse, and internal controls codified in Title 31 United States Code. This information is shared with the third parties using a SOAP-based web service call.

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

The PII in Genesis is retained and disposed under the requirements of the National Archives and Records Administration (NARA) General Records Schedule GRS 1.1: Financial Management and Reporting Records Schedule.

## 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 information in Genesis is protected by the FCC's privacy controls that include a comprehensive and dynamic set of safety and security protocols that are designed to meet all Federal privacy standards, including those required by the National Institute of Standards and Technology (NIST) and the Federal Information Security Modernization Act of 2014 (FISMA). The protocols cover all electronic records, including those housed at the FCC and those information systems that are housed at the FCC's authorized contractors. There are a limited number of paper records that are stored in file

cabinets in the FO office that are locked when not in use and/or at the end of the business day. These paper documents are maintained for short periods as needed and then destroyed. All access points for the FO office suite are monitored.

**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.**

No.

## 1.6. Access to the Information

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

Only authorized FCC supervisors, employees, and contractors have access to the electronic records and paper document files.

**B. Does this system leverage Enterprise Access Controls?**
Yes. Genesis uses OKTA for access control.

**C. Does the system leverage the FCC's Accounting for Disclosure control?**
Yes.

# Appendix A - Acronyms and Abbreviations

[Populate based upon abbreviations used in the document. ]

**Table A-1: Acronyms and Abbreviations**

| Acronym | Definition |
|---|---|
| API | Application Programming Interface |
| ATO | Authority to Operate |
| COTS | Commercial Of The Shelf software |
| CSRS | Computer Security Resource Center |
| DOJ | U.S. Department of Justice |
| EIN | Employee Identification Number |
| FCC | Federal Communications Commission |
| FedRAMP | Federal Risk and Authorization Management Program |
| FO | Financial Operations |
| GRS | General Records Schedule |
| ID | Identification |
| IP | Internet Protocol |
| IPA | Initial Privacy Assessment |
| ISSO | Information System Security Officers |
| IT | Information Technology |
| MAC | Media Access Control |
| NARA | National Archives and Records Administration |
| NFC | National Finance Center |
| NIST | National Institutes of Standards and Technology |
| OMB | Office of Management and Budget |
| OMD | Office of the Managing Director |
| PaaS | Platform as a Service |
| PIA | Privacy Impact Assessment |
| PII | Personally Identifiable Information |
| POC | Point of Contact |
| SaaS | Software as a Service |
| SAOP | Senior Agency Official for Privacy |
| SORN | System of Records Notice |
| USDA | U.S. Department of Agriculture |