UNITED STATES

FEDERAL COMMUNICATIONS COMMISSION

# PRIVACY IMPACT ASSESSMENT (PIA) FOR MONSTER HIRING MANAGEMENT ENTERPRISE (MHME) PART OF THE ESI SAAS - 2 BOUNDARY

December 2022

OFFICE OF GENERAL COUNSEL

Washington DC, 20554

## Next Review Cycle:

**December 2023**

## Record of Approval

| | | |
|---|---|---|
| **Document Approval** | | |
| **Drafter Name: Caleb Laster** | | **Bureau/Office: OMD/IR** |
| **SAOP Approval** | | |
| **Printed Name:** Elliot S. Tarloff | | **Senior Agency Official for Privacy** |
| **Signature:**<br>Elliot S. Tarloff Digitally signed by Elliot S. Tarloff Date: 2022.12.14 14:43:43 -05'00' | **Date** | |

## Record of Approval

| Date | Description | Author |
|---|---|---|
| 10/03/2022 | Validation of information – System Owner | Diana Huynh |
| 10/05/2022 | Validation of completeness – IT Compliance Representative in lieu of IT Compliance Lead | Hans Agarwal |

## Revision History

| Date | Description | Name |
|---|---|---|
| 10/05/2022 | Original Document Created | Caleb Laster - ISSO |
| 10/21/2022 | Revisions by Privacy Team | Privacy Legal Advisor – Katherine Morehead;<br>Senior Agency Official for Privacy (SAOP) – Elliot S Tarloff |
| 11/01/2022 | Formatting revisions and edits to Sections 1.2, 1.3B, 1.4A, and 1.6A | SAOP |
| 12/06/2022 | Revisions to Sections 1.2, 1.3B, 1.3D, and 1.6A. | Privacy Legal Advisor & SAOP |

# MONSTER HIRING MANAGEMENT ENTERPRISE (MHME) part of THE ESI SAAS-2 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**<br>Monster Hiring Management Enterprise (MHME) |
| **NAME OF BUREAU**<br>Office of the Managing Director (OMD) |
| **DOES THE SYSTEM CONTAIN PII?**<br>Yes. MHME contains PII from job applicants to the FCC, and records are retrievable and retrieved from MHME using the names (or other unique identifiers) of individual job applicants. |
| **PLEASE PROVIDE A BRIEF DESCRIPTION OF THE PII (IF APPLICABLE)**<br>The data fields collected from Job Seekers are:<br>• Full name: first, middle or initial, last<br>• Home address<br>• E-mail address<br>• Telephone Numbers<br>• Citizenship/Nationality Information<br>• Race and/or other demographic information (if provided)<br>• Attached documents include: Resume, cover letters, transcripts, proof of veteran status, and/or proof of federal agency status |
| **IN WHAT SYSTEM OF RECORDS (SORN) IS THE INFORMATION CONTAINED (IF APPPLICABLE)?**<br>OPM GOVT-5 |
| **WHAT ARE THE LEGAL AUTHORITIES FOR THE COLLECTION OF THIS PII?**<br>The Privacy Act of 1974 (5 U.S.C. § 552a); 5 U.S.C. §§ 1302, 3109, 3301, 3302, 3304, 3305, 3306, 3307, 309, 3313, 3317, 3318, 3319, 3326, 4103, 4723, 5532, and 5533; and Executive Order 9397. |
| **DOES THE COMMISSION KEEP AN ACCURATE ACCOUNTING OF DISCLOSURES FROM THE** |

| |
|---|
| **SYSTEM AS REQUIRED BY SUBSECTION (C) OF THE PRIVACY ACT?**<br>Yes. |
| **DOES THIS SYSTEM SHARE THE PII WITH OTHER SYSTEMS?**<br>No |

**Is this a new ATO Boundary or an existing ATO Boundary?**

☐ New Boundary
☒ Existing Boundary

A. **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)

☐ 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) [list applicable system(s)]

B. **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 carry out the purpose of each of the system(s) that maintain PII within this Boundary.**

The FCC is required to post vacancies for federal employment on USA Jobs (www.usajobs.gov), which is operated and maintained by the Office of Personnel Management (OPM). The FCC will employ the MHME system to facilitate recruitment at the FCC. FCC HR will administer this

[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.

module for its job vacancies. Developed as a Software-as-a-Service (SAAS) by Monster, this system may be utilized on demand by FCC employees and contractors for recruiting purposes.

### 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.

PII will be collected directly from job seekers themselves. The FCC's instance of the MHME system provides a Privacy Act Statement at the point of collection, which includes the following:

**Purpose:** FCC collects Personally Identifiable Information from Federal Job Applicants to automate Human Resource and recruitment activities. Applicant information such as professional resumes, contact information, and supporting documentation is collected in support of the job application process.

**Routine Uses:** FCC collects and stores only the information required for candidate recruitment, selection, and onboarding for federal employment, in accordance with the laws and regulations governing such activity. The information will be disclosed to and used by authorized FCC personnel, its fiscal and financial agents, and other federal agencies, as necessary to complete your entrance on duty for Federal employment.

**Disclosure:** Providing this information is voluntary, however, your application or entrance on duty cannot be processed without it.

**Request For Information on Records:** Applicants seeking information on their own records owned and maintained by FCC can contact the hiring agency in accordance with the applicable System of Records Notice (SORN), OPM Govt 5 SORN.

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

The system will collect only the data necessary to communicate with job applicants and verify the suitability of applicants to fill the FCC roles to which they have applied.

### 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 individuals providing the data to ensure the completeness, accuracy, and currency of information at the time it is submitted within the FCC instance of the MHME. Information that is used by the FCC as part of its HR recruitment and other activities will

[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.

be reviewed for accuracy and timeliness as required by the particular activity and the laws and authorities, if any, applicable at the time the agency compiles the records (e.g., Communications Act, personnel laws, administrative or court evidentiary rules and procedures). The integrity of the PII is maintained by retrieving the PII using AD accounts (for User ID and password) and the general FCC HR System using Secure File Transfer Protocol (SFTP) feeds.

## 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?**

Job applicants submit their PII to the MHME through the public-facing website. Data obtained from applicants enter the MHME boundary from public internet connections that leverage Secure Shell (SSH) for File Transport Protocol (FTP) or Hypertext Transfer Protocol Secure (HTTPS) for web services.

FCC HR users will log into the web-based application with their FCC credentials to view the information from applicants. Once an applicant is selected by the selecting official and depending on the type of FCC vacancy, various business units within the FCC will have access to the relevant PII related to the applicant. The FCC Human Resources Management, Recruitment and Staffing Service Center, Administrative Staff in the Bureau Offices and Executive Resources Group will have access to the PII maintained within the FCC MHME instance.

The MHME System leverages Secure File Transport Protocol (SFTP) feeds. A CSV file from the SFTP feed which contains MHME, and AD user information is sent twice a week (Tuesday and Friday) to the FCC MHME instance. This connection will be reflected in CSAM when MHME is stood up in CSAM. Using both AD and MHME, the list of employees and contractors who may have access to the FCC technology systems are listed in MHME to ensure all are accounted for.

**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")?**

The information will not be shared with third parties as part of the operations of the information system through an API.

**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, privacy controls are included in the FedRAMP package**.**

## 1.6 Access to the Information

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

The FCC Human Resources Management, Recruitment and Staffing Service Center, Administrative Staff in the Bureau Offices and Executive Resources Group will have access to the PII maintained within the FCC MHME instance. Additionally, any FCC employee that serves in a capacity that would require him or her to recruit, interview, and or participate in the onboarding of selected applicants may obtain or view some form of the PII within the MHME.

## B. Does this system leverage Enterprise Access Controls?

Yes, this system uses the FCC AD for access, which leverages Okta for login and authentication, AD for user-details, integration, and access. The FCC also ensures only required admins and internal users will have access to the FCC MHME system.