UNITED STATES

FEDERAL COMMUNICATIONS COMMISSION

PRIVACY IMPACT ASSESSMENT (PIA) FOR THE SAP NS2 SUCCESSFACTORS HCM SUITE SYSTEM (ESI-SAAS (2)) FISMA FCC BOUNDARY

August 2022
Annual Review Date

OFFICE OF GENERAL COUNSEL

Washington DC, 20554

Next Review Cycle: August 2023

Record of Approval

Document Approval		
Drafter Name: Curtis Everett / Ryan Washington		**Bureau/Office: OMD/IR**
SAOP Approval		
Printed Name: Elliot S. Tarloff		**Senior Agency Official for Privacy**
Signature: Elliot S. Tarloff Digitally signed by Elliot S. Tarloff Date: 2022.08.10 16:29:49 -04'00'	**Date**	

Record of Approval

Date	Description	Author
07/25/2022	Validation of information – System Owner	Curtis Everett / Ryan Washington
08/09/2022	Validation of completeness – IT Compliance Representative in lieu of IT Compliance Lead	Hans Agarwal

Revision History

Date	Description	Name
08/09/2022	Original Document Created	ISSO/Privacy Team

SAP N2 SuccessFactors HCM Suite 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 SAP NS2 SuccessFactors HCM Suite (SAP SuccessFactors)
NAME OF BUREAU Office of the Managing Director (OMD)
DOES THE SYSTEM CONTAIN PII? Yes. The PII of FCC employees and contractors may be retrieved from Active Directory (AD) accounts.
PLEASE PROVIDE A BRIEF DESCRIPTION OF THE PII (IF APPLICABLE) PII elements retrieved from AD include name, work email address, and other employment records and information.
IN WHAT SYSTEM OF RECORDS (SORN) IS THE INFORMATION CONTAINED (IF APPPLICABLE)? OPM GOVT-1
WHAT ARE THE LEGAL AUTHORITIES FOR THE COLLECTION OF THIS PII? Pursuant to 5 U.S.C. 4118, the Office of Personnel Management (OPM) requires federal agencies to maintain general personnel records about their staff, including records relating to government-sponsored training.
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? Yes, while there are no APIs, there are feeds from AD and Human Resources Management (HRM) system into other systems using an SFTP feed. A CSV file is transmitted via SFTP that contains HRM & AD user information twice a week (Tuesday and Fridays) to other systems.

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

☒ New Boundary - (SAP is a new system in the FISMA FCC ESI SaaS(2) 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:

FCC will employ the Learning Management System (LMS) module of the SAP SuccessFactors system. FCC University will administer this module for its repository of training courses. Developed as a Software-as-a-Service (SAAS) by SAP, this module may be utilized on demand by FCC employees and contractors for training purposes.

☒ The FCC uses provider-supported application/s on the provider's cloud network (Software as a Service or SaaS) [list applicable system(s)]: SAP SuccessFactors LMS Module – This is a Software-as-a-Service system that is hosted on the AWS platform.

☐ 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

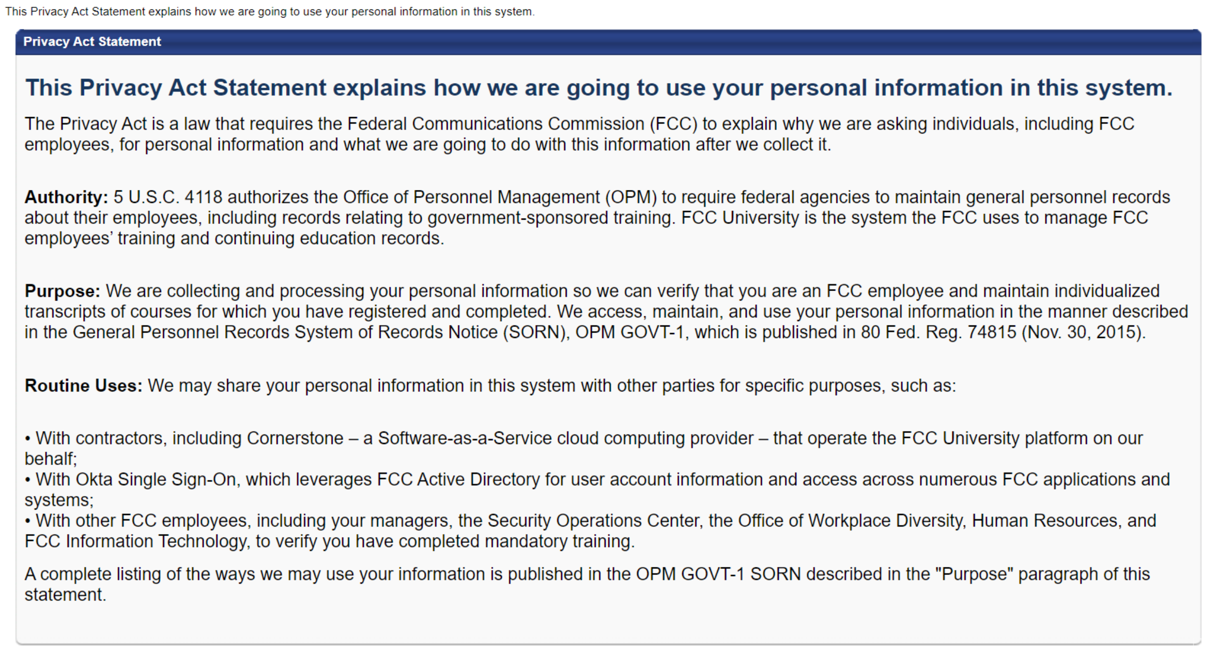
[3] *See* NIST, *The NIST Definition of Cloud Computing*, Special Pub. No. 800-145 (Sep. 2011), https://csrc.nist.gov/publications/detail/sp/800-145/final.

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.**
Pursuant to 5 U.S.C. 4118, the Office of Personnel Management (OPM) requires federal agencies to maintain general personnel records about their staff, including records relating to government-sponsored training.

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.** Yes, SAP SuccessFactors collects information from individuals themselves. See Privacy Act Link and Screenshot below:

Privacy Act Statement Template (dhs.gov)



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

Privacy Act Statement

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

The Privacy Act is a law that requires the Federal Communications Commission (FCC) to explain why we are asking individuals, including FCC employees, for personal information and what we are going to do with this information after we collect it.

Authority: 5 U.S.C. 4118 authorizes the Office of Personnel Management (OPM) to require federal agencies to maintain general personnel records about their employees, including records relating to government-sponsored training. FCC University is the system the FCC uses to manage FCC employees' training and continuing education records.

Purpose: We are collecting and processing your personal information so we can verify that you are an FCC employee and maintain individualized transcripts of courses for which you have registered and completed. We access, maintain, and use your personal information in the manner described in the General Personnel Records System of Records Notice (SORN), OPM GOVT-1, which is published in 80 Fed. Reg. 74815 (Nov. 30, 2015).

Routine Uses: We may share your personal information in this system with other parties for specific purposes, such as:

- With contractors, including Cornerstone – a Software-as-a-Service cloud computing provider – that operate the FCC University platform on our behalf;
- With Okta Single Sign-On, which leverages FCC Active Directory for user account information and access across numerous FCC applications and systems;
- With other FCC employees, including your managers, the Security Operations Center, the Office of Workplace Diversity, Human Resources, and FCC Information Technology, to verify you have completed mandatory training.

A complete listing of the ways we may use your information is published in the OPM GOVT-1 SORN described in the "Purpose" paragraph of this statement.

[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.

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 verify an employee's identity and to create a record of training for each employee that uses the system.

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

PII data is retrieved from AD accounts (for User ID and password) and the general HRM System using Secure File Transfer Protocol (SFTP) feeds. A Comma-Separated Values (CSV) file from the SFTP feed which contains HRM & AD user information is sent twice a week (Tuesday and Fridays).

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?

PII is retrieved from AD accounts (for User Id and password) and the general HRM System using SFTP feeds. A CSV file from the SFTP feed which contains HRM & AD user information is sent twice a week (Tuesday and Friday). This connection will be reflected in CSAM when SuccessFactors is stood up in CSAM. Using both AD and HRM, the list of employees, contractors, and vendors who may have access to the FCC technology systems are listed in SAP SuccessFactors to ensure all are accounted for. Results from training and education is sent from SAP SuccessFactors as a CSV file via SFTP. The system does not have any direct connections through API or other means to any 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?

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?

HR, IT Training Specialists, and other external contractors responsible for learning management.

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 system sits behind the

FedRAMP network security validated controls. FCC also ensures only required admins and internal users will have to SAP SuccessFactors.