U.S. DEPARTMENT OF JUSTICE
Federal Bureau of Prisons

PROGRAM STATEMENT
Federal Prison Industries
Financial Information System Authorizations

Approved by	William K. Marshall III Director, Federal Bureau of Prisons
DPI	FPI
Number	8052.04
Date	March 19, 2026

Summary of Changes

Program Statement Rescinded: ▪ 8052.03 Millennium Authorizations (3/19/15)
Changes: ▪ Updated terminology to reflect changes to the financial information system used by Federal Prison Industries (FPI).

1. **PURPOSE AND SCOPE**

To establish standards for creating and maintaining access authorizations in the FPI financial information system (currently SAP S/4HANA).

a. **Program Objectives.**

- Clearly defines roles and responsibilities for the development, maintenance, and assignment of user authorizations in the FPI financial information system.
- Security of information in the FPI financial information system will be maintained by proper internal controls.

b. **Institution Supplement**. None.

2. **RESPONSIBILITIES**

This section defines the roles and responsibilities of the following positions within FPI:

3

a. **Business Process Owners** (BPO). The functional personnel responsible for protecting the integrity of the information and processes supported by the FPI financial information system. BPOs or designees are responsible for:

- Developing and approving written mitigating controls for segregation of duty (SOD) risk identified by the Governance, Risk, and Compliance (GRC) tool.
- Approving newly created or changes to existing roles in their functional area.
- Reviewing and approving the re-certification of the functional roles assigned to users.

b. **Deputy Assistant Director (DAD).** The person responsible when mutual agreement cannot be reached by the granting BPO and requestor, the DAD makes the final decision based on all the information given to them to grant or deny the request.

c. **Enterprise Resource Planning (ERP) Help Desk.** ERP Help Desk personnel are responsible for monitoring, directing, and developing FPI financial information system access. This includes but is not limited to:

- Role creation, maintenance, and deletions based upon BPO approval.
- Maintaining license controls for users, and providing ad hoc license reports to all business areas, as well as the final yearly license report to SAP.
- Preparing the annual recertification documents for user accounts.
- Reviewing requests for new FPI financial information system users and modifications to existing accounts, coordinating the approval process of all stakeholders, and issuing direction to the SAP User Administrator in making the actual user account change.

d. **ERP Business Process Analysts.** ERP duties are to help administrators define the technical rules for each business area for approved risk conditions and recommend alternatives to eliminate SOD risks in roles and user assignments.

e. **Internal Control and Compliance Group (ICCG).** ICCG performs risk assessments and mitigating control reviews on a regular basis to identify new risks, performs periodic testing of rules and mitigating controls, and acts as a liaison with external auditors.

f. **GRC Administrator.** The GRC Administrator maintains the GRC tool. This includes but is not limited to the following functions:

- Maintaining and managing the GRC tool.
- Primary gatekeeper of SOD compliance and reporting among roles and user accounts.
- Maintaining GRC mitigating control (MC) documentation.
- Maintaining GRC reports or monitoring tools to identify SOD conflicts and user access.

g. **SAP Security Administrator.** The SAP Security Administrator maintains security

3

procedures for the SAP environment. This includes but is not limited to:

- Developing SAP security procedures and monitoring methods.
- Using the GRC tool to monitor the SAP environment for SOD compliance and reporting among roles and user accounts.
- Using the GRC tool to monitor MCs.
- Reviewing the role development process and advising about security concerns.

h. **Information System Security Officer (ISSO).** This is a Management Information Systems Branch (MISB) position and is responsible for security policy compliance throughout FPI. They perform audits and generate reports on system security violations to the Department of Justice (DOJ) and FPI management. This position also tracks violations and system security changes.

i. **SAP User Administrator.** This position is responsible for creating and maintaining user accounts. They are typically the System Administrator, but the duties can be assigned to other positions or automated systems.

j. **License Owners (LO).** Individuals or entities who have authority over the SAP access licenses for a specific business process or business group (e.g., branch chiefs).

k. **Chief Information Officer** (**CIO).** The individual responsible for all information system matters. The CIO is responsible for System Administrators. ERP is also a section within MISB.

l. **Chief Financial Officer (CFO)**. The individual with ultimate responsibility for financial policy and procedure.

m. **Branch Chief (BC) or General Manager (GM)**. Individual responsible for a support branch or business unit within FPI. The BC or GM (or designee) is responsible for user license approval for new users in their unit.

n. **Chief Enterprise Resource Planning** (**CERP).** The individual with ultimate responsibility for all aspects of FPI financial information system authorizations. When a decision made for a role or the abuse of role privileges introduces a threat to the security of the FPI financial information system environment, the CERP has the authority to overrule the decision to eliminate or reduce the threat.

3. FPI FINANCIAL INFORMATION SYSTEM LOGON ACCOUNT

Staff, contractors, vendors, and inmates granted access to FPI's financial information system are issued only one logon account per person.

4. FPI FINANCIAL INFORMATION SYSTEM USER ACCOUNT CHANGES

a. **Assignment of Roles.** It is through the approval of the BPO that users are approved to use a role to perform a specific task within FPI's financial information system.

Each user account is validated to ensure segregation of duties (SOD) conflicts are identified and mitigated within the FPI financial information system using the GRC tool.

The role is assigned by the SAP User Administrator to the SAP user account. Staff are assigned to approved roles ending with "*staff"* or *"st"* and inmates are assigned to approved roles ending with "*inmates"* or *"in".*

Functional roles are named and assembled based on specific functions required for a specific job performance. For example, the activity group "*Acct*" contains the transactions required to perform an Accountant's duties and responsibilities.

The Temporary Access call type in the help desk service ticket system is used when roles assigned either as collateral duty or on a temporary basis result in an SOD conflict. The user request is approved or disapproved, and the mitigating control approval is completed by the BPO.

b. **Users Departing FPI.** The SAP User Administrator secures the account when notified that a user is separating or has separated from FPI by:

- Removing all roles and profiles from the account.
- Setting the account's user group to "expired."
- Setting the account's "valid through date" to the current system date.
- Setting an administrative lock on the account.

c. **Users Transferring to Another FPI Facility.** For users who are transferring to another FPI location, the sending SAP User Administrator modifies the account as follows:

- Removing all roles and profiles from the account.
- Setting an administrative lock on the account.

The receiving SAP User Administrator at the new location makes the appropriate assignments based on the new supervisor's request, BPO approval, and as directed by the ERP Help Desk.

d. **Requesting Changes to Existing Authorizations.** When an individual user needs authorization to perform a transaction that their assigned role does not permit, they should follow the proper chain of command to submit a help desk service ticket.

3

If the authorization cannot be provided through assignment of an existing role, a role modification or new role creation must be initiated. To initiate this change, the pre-existing help desk service ticket is approved by the BPO. The help desk service ticket is closed out and becomes a system change request (SCR) in the Enterprise Change Management System. The approved changes are completed following the Standard Operating Procedure System Development Life Cycle (SDLC) for ERP Systems. Changes to user accounts as the result of the SCR process are carried out by the SAP User Administrator via instructions from the SAP Access Administrator help desk service ticket.

e. **Annual User Account Recertification.** Recertification requires that every role assigned to a user account is reviewed and approved annually by the functional BPO. Changes to user accounts as a result of the recertification process are carried out by the SAP User Administrator via instructions from the SAP Access Administrator.

f. **Annual BPO Account Recertification.** Recertification requires that every role assigned to a BPO account is reviewed and approved annually by the primary BPO or DAD. Changes to a BPO account as a result of the recertification process are carried out by the SAP User Administrator via instructions from the SAP Access Administrator.

5. SEGREGATION OF DUTIES (SOD).

SOD conflicts are risks or transactions that present an opportunity for an individual to control a process, from beginning to end, without the involvement of others.

The process of segregating is the ability to separate out transactions within a role, or the stacking of roles to eliminate the threat of an individual controlling an entire process, as a matter of security and/or internal control management.

SOD conflicts are identified using the GRC tool maintained by the GRC Administrator or designee. A role or user account with a combination of roles that present SOD conflicts are reported to the BPO to either:

- Assign an existing mitigating control.
- Create a new mitigating control.
- Remove the role or transaction causing the conflict.

a. **Mitigating Controls (MC).** This is action taken to monitor activities when a business condition requires personnel to have the opportunity to exploit operational weakness through additional access to FPI's financial information system.

BPOs are responsible for writing MCs to monitor a conflict. The MCs should:

3

- Identify how the risk is specifically monitored.
- Identify how often the risk is monitored.
- Identify who or what tool is responsible for conducting the monitoring task.
- List the potential violations the monitoring task should identify.

The ICCG reviews MCs for accuracy and compliance with current policies.

An approved MC is submitted to the GRC Administrator. This position is responsible for:

- Maintaining approved MC documentation.
- Inputting approved MC into the GRC tool.
- Assigning users to MCs within the GRC tool.
- Maintaining the BPO listings and monitoring listings within the GRC tool.
- Notifying BPOs of any unmitigated SOD conflicts.
- Generating SOD audits and general reports.

b. **Annual Mitigating Controls Recertification.** BPOs must review the MCs report for all known controlled risks at least annually to maintain compliance with policy and consistency within the FPI financial information system environment.

The GRC Administrator executes a SOD user report without mitigating risk. The BPO identifies the MC to apply or which role to remove for each listed user account that has conflicts.

Changes to user accounts as the result of the recertification process are carried out by the SAP User Administrator via instructions from the SAP Access Administrator help desk service ticket. Changes to the GRC tool, as the result of the recertification process, are carried out by the SAP Security Administrator.

6. INCIDENT RESPONSE

Violations to the procedures listed in this program statement are investigated, and when deemed necessary by FPI's ISSO are reported in accordance with FPI's Incident Response Plan.

REFERENCES

Program Statements
FPI Standard Operating Procedures
System Development Life Cycle (SDLC) for ERP Systems

ACA Standards
Performance-Based Standards and Expected Practices for Adult Correctional Institutions (5th Edition): 5-ACI-7A-12

Performance-Based Standards and Expected Practices for Adult Local Detention Facilities (5th Edition): 5-ALDF-5C-16

Standards for the Administration of Correctional Agencies, 2nd Edition: 2-CO-1F-06

Records Retention Requirements
Requirements and retention guidance for records and information applicable to this policy are available in the Records and Information Disposition Schedule (RIDS) on the Bureau's intranet site.