

**U.S. DEPARTMENT OF JUSTICE
Federal Bureau of Prisons**



**PROGRAM STATEMENT
Federal Prison Industries Information Technology Systems
Administration**

Approved by	 William K. Marshall III Director, Federal Bureau of Prisons
DPI	FPI
Number	8051.05
Date	September 3, 2026

Summary of Changes

<i>Program Statement Rescinded:</i> 8051.04 UNICOR Information Technology Systems Administration (03/18/2015)
<i>Changes:</i> - Updates information on storage of back up data. - Updates sections on document management and training.

1. PURPOSE AND SCOPE

To define standards for the management of Federal Prison Industries' (FPI) information technology (IT) systems and resources and their administration.

This program statement establishes standards that govern the life cycle management of FPI's IT hardware and software systems and defines procedures for effective management of IT resources. It provides a mechanism for rapidly incorporating new IT standards established by the Department of Justice (DOJ) or other federal IT regulatory authorities.

With the exception of security oversight and vulnerability management by the Chief Information Security Officer (ISO), this standard does not apply to FPI "production" systems. Production systems include any hardware, software, or combination thereof used for task-specific purposes. Production systems include any hardware or software configured and used specifically to satisfy the requirements of an FPI contract or those systems required by a customer for the production of goods or services under a contract.

a. **Program Objectives.**

- Software and data stored on FPI's computer systems will be properly safeguarded.
- Computer resources will be effectively managed and protected from environmental damage and unauthorized access.
- System Administrators (SA) will be adequately trained to support FPI's information technology network and provide technical assistance to staff.

b. **Institution Supplement.** None.

2. **ROUTINE PROCEDURES**

To ensure IT systems and data are protected, the Management Information Systems Branch (MISB) has identified standard controls and corresponding operational and configuration standards.

a. **FPI IT Standard Controls** define requirements that apply to all data centers, systems, staff, or resources throughout FPI. These include:

- Account Management.
- Data Management.
- Change Management.
- Environmental Controls.
- Vulnerability Management.

b. **MISB Operational and Configuration Standards** are technical reference guides that define specific system configuration procedures, system specifications, or standards that govern IT resource management practices to which SAs must conform. Technical reference documents may apply to MISB as a whole or only to specific practices of different sections within MISB. MISB standards include:

- SAP standard operating procedure.
- Applications development standards.
- Field procedures and systems standards.
- E-commerce electronic data interface standards.
- ISM operating procedures and configuration standards.

FPI standard controls and MISB technical reference guides ensure:

- Access to systems is controlled and documented.
- Systems are configured correctly.
- Security systems/protectations are implemented properly.

- Systems are maintained correctly so that daily operations are not adversely affected.
- Data accuracy and accessibility is ensured.
- System performance is routinely monitored and reported.

Performance of those tasks ensures:

- Critical data is properly backed up.
- System logs are reviewed for any abnormal events and resolved.
- Users are prevented from accessing restricted resources or sensitive data.
- The current system is performing optimally.

3. INFORMATION TECHNOLOGY GENERAL CONTROLS

FPI systems and business data integrity must be protected at all times. Critical systems must be properly secured in locations that address environmental issues, such as power and ventilation, fire prevention, and disaster recovery.

- a. **Computer Room and Data Closet Access.** Each computer room and data closet must have a secure lock on the door; access is restricted to authorized staff. An Access Control List is posted at the entrance to these spaces. Under no circumstances may doors to these spaces be left open unattended.
- b. **Environmental Conditions.** Environmental conditions must be monitored to prevent damage. Each location or data center ensures that environmental control equipment is installed to maintain industry-recommended temperatures and relative humidity.
- c. **Computer Room Construction.** The Program Statement **Factory Construction and Activation Manual – FPI** contains detailed specifications for new computer room construction. Staff at existing institutions ensure new computer rooms comply with these standards.
- d. **Data Management.** System backups are performed frequently. Backup data is stored at offsite secure locations or in the cloud in an availability zone separate from the original source data. SAs must be familiar with backup software and procedures used to restore data.
- e. **Systems and Software Maintenance.** Hardware, operating system, and application updates are applied in a timely manner. Operating system and application patches are tested and documented using non-critical or non-production systems before being applied to any production system.
- f. **Access Control.** Access control procedures protect systems from unauthorized physical and logical access. They ensure or validate that a system user has received proper clearance and has

supervisory approval before access, and that control measures are documented. Access control procedures apply to any means of access to FPI's systems and to any system owned by FPI.

g. **System Refresh.** MISB establishes a hardware/software refresh cycle to distribute the costs of replacing aging hardware and software over several years. Funding is requested in each fiscal year cycle, subject to approval by FPI corporate management and FPI's Board of Directors.

h. **System Development Life Cycle (SLDC)/Change Control.** FPI complies with SDLC and change control policies defined by the DOJ.

i. **Audit/Program Review.** MISB ensures applicable general control and Information Technology Systems Standards (ITSS) security standards are followed through periodic internal reviews.

j. **SAs.** MISB directs SAs providing IT support at factory locations and in the Central Office. SAs also participate in temporary duty assignments away from their primary support locations in direct support of FPI operations. The SA serves as the Information Security Officer (ISO) for the FPI factories they support. Their security responsibilities are defined by the DOJ to the extent they do not violate segregation of duty policies. The FPI Chief ISO in the Central Office has overall security oversight within FPI, as delegated by the Chief Information Officer.

4. **DOCUMENT MANAGEMENT**

MISB Section Chiefs annually review standards and guides to ensure they remain current. Printed copies may be maintained but must be protected from unauthorized staff or inmate access.

MISB updates technical reference guides to address improvements in technology and procedures. SAs are notified via email when updates are made.

5. **TRAINING**

MISB staff are provided training opportunities to the fullest extent possible. Technological requirements, policy, or security mandates are the basis for providing training. The needs of the organization and the employee's ability to perform their duties are considered when determining whether training should be provided.

6. **ASSISTANCE**

Direct questions to the Chief Information Officer, MISB.

REFERENCES

Program Statements

Factory Construction and Activation Manual – FPI

ACA Standards

Evidence-Based Standards and Expected Practices for Adult Correctional Institutions (5th Edition): 5-ACI-1F-07

Evidence-Based Standards and Expected Practices for Adult Detention Facilities (5th Edition): 5-ALDF-7D-29

Standards for Administrative Administration of Correctional Agencies (2nd Edition): 2-CO-1F-06

Records Retention Requirements

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