


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



**PROGRAM STATEMENT  
Office of Security Technology**

Approved by	 William K. Marshall III Director, Federal Bureau of Prisons
DPI	ITDD
Number	1150.07
Date	March 19, 2026

**Summary of Changes**

<i>Program Statement Rescinded:</i> <ul style="list-style-type: none"><li>1150.06 Office of Security Technology (4/05/2013)</li></ul>
<i>Changes:</i> <ul style="list-style-type: none"><li>Updates division responsible for the Office of Security Technology.</li><li>Modifies form name from OST Technology Evaluation to Security Technology Evaluation.</li><li>Updates terminology and acronyms.</li><li>Removes attachment.</li></ul>

**1. PURPOSE AND SCOPE**

To establish the duties and responsibilities of the Office of Security Technology (OST). This office is a branch within the Information, Technology, and Data Division (ITDD).

**a. Program Objectives.**

- Appropriate technology solutions will be introduced to the Bureau through a program of technology assessment and operational evaluation.
- Technical issues beyond the routine duties and expertise of institutional staff will be resolved by OST staff.
- OST subject matter experts will be provided as needed to offices outside of Central Office (e.g. regional offices, institutions).
- Resources of other federal, state, county, and foreign law enforcement agencies will be used to improve staff expertise in technology areas by exchanging information.
- Security technology issues requiring research and development expertise, or funding will

be coordinated by OST and transferred for evaluation to the appropriate Department of Justice (DOJ), Department of Defense (DOD), or other governmental organization upon approval of the Assistant Director (AD), ITDD.

- Through dissemination of OST formal evaluations, when appropriate, or other technology evaluation and reporting formats, to the National Institute of Corrections (NIC) or the National Institute of Justice (NIJ), OST will enhance collaboration with other federal, state, and local organizations.

b. **Institution Supplement.** None.

## 2. RESPONSIBILITIES

OST is responsible for identifying new security-related technology and equipment, evaluating its potential use and effectiveness, and assisting in its implementation. OST is also responsible for approving any security technology purchase over \$5,000.

The Office of Security Technology performs the following functions to support field security operations:

a. **Identifies and screens.** Identifies and screens new security equipment and technology with potential for Bureau use. Selection of technologies for review is based upon security priorities identified by the Executive Staff and field requests for evaluation of specific technology solutions to security problems. OST is not a research and development organization but conducts operational evaluations of potential technology solutions to Bureau security issues.

b. **Coordinates evaluations.** Coordinates operational evaluations with the relevant discipline of new security technology products with potential for significant field application. Multiple products are assessed to identify characteristics necessary to ensure effective use of the technology.

“Operational evaluation” is defined as the test and analysis of a specific technology or system, as far as practicable under operating conditions, to determine if it should be adopted for Bureau use, considering the increase in correctional effectiveness to be gained, and its effectiveness as compared with currently available devices or systems. Consideration is given to:

- Personnel capabilities to maintain and operate the equipment.
- Size, weight, cost, and location considerations.
- Measurable operational effectiveness in field institutions.

c. **Prepares evaluations.** Prepares an operational evaluation for the Executive Staff or appropriate requester that follows the parameters of the BP-A1008, Security Technology

Evaluation Template. If appropriate, the report includes a draft memorandum from the AD, ITDD to the field recommending the purchase of the technology and any other relevant product information.

d. **Establishes standards.** Establishes initial Bureau-wide standards for use of new technology systems. Once a technology is adopted for Bureau use, the respective division for the discipline using the technology is responsible for updating Bureau-wide standards for that technology.

e. **Establishes liaisons.** Establishes liaisons with other federal, military, and state law enforcement or correctional agencies and with other organizations to share knowledge and obtain assistance to evaluate new technologies.

### 3. STAFF ASSISTANCE AND REVIEW VISITS

OST staff may be sent to any institution during or after a significant incident in which technology was involved or could be part of an appropriate response. OST staff may be appointed to after-action review teams to:

- Determine whether any failure occurred in security equipment or systems.
- Identify the cause of a failure.
- Make recommendations to prevent recurrence.

OST staff are available for onsite review of specific security problems. If a Warden determines assistance is required to identify a technological solution for a problem, or an innovative application of existing technology is needed, a request for OST assistance may be made through the Regional Director to the AD, ITDD. When approved, OST assistance is coordinated with institution staff as well as regional and Central Office administrators.

### 4. SECURITY TECHNOLOGY OPERATIONAL EVALUATION PROJECTS

Based upon AD, ITDD, recommendation and Executive Staff approval, OST may fund a limited number of field operational evaluations each year. Operational evaluations selected for funding are evaluated in an institution setting. Such projects are coordinated with regional and Central Office administrators.

When possible, local staff who initiate a project are involved in the operational evaluation. OST prepares a written, agreed-upon plan of action including:

- Institution responsibilities.
- Institution staff requirements.
- Points of contact.

- Evaluation criteria.

When warranted, OST formulates evaluation plans supporting a consistent approach to evaluating new security technologies and strengthen Bureau decisions about deploying pilot projects. Such plans may include defining measurable objectives and a detailed data analysis plan. However, many technologies do not lend themselves to a formal evaluation plan or detailed data analysis plan.

A simple evaluation may consist of OST or field subject matter experts ensuring equipment functions as described in the marketing materials or reviewing existing evaluations of new technology conducted by a recognized military, law enforcement, or corrections organization. If warranted, OST employs an evaluation template which is the BP-A1008, Security Technology Evaluation Template that can be used in more formal evaluations. Evaluation-related responsibilities are coordinated with institution management to ensure testing duties do not interfere with operational responsibilities.

For products tested in an institution, the Warden sponsors and provides staff to coordinate the project at the institution level.

Project staff submit periodic operational evaluation reports to OST. The frequency and format of reports may vary, depending on the project's duration and scope.

Upon project completion, OST, with input from project staff, prepares documentation describing the results and making recommendations for the equipment/system's future use.

Priority is given to projects based on the following criteria:

- Broad application among institutions.
- Potential to reduce life-threatening security risks to staff and inmates.
- Potential to improve overall security effectiveness.
- Cost-effectiveness.

Any Central Office branch, regional office, or institution may submit a project for consideration using the BP-A1008, Security Technology Evaluation Template. The form must be signed by the Warden, Regional Director, or appropriate AD and submitted to the AD, ITDD.

## 5. PROCEDURES FOR OPERATIONAL EVALUATION OF TECHNOLOGIES

a. **Screening.** OST reviews new security products with potential Bureau use to determine whether further evaluation is appropriate. While OST communicates with other law enforcement agencies and suppliers regularly, it is impossible for a single entity to screen all information

resources for technology products that may improve institution security. Therefore, staff are encouraged to report new technologies to OST for further evaluation. When practical, OST evaluates new equipment/systems before operational evaluation.

b. **Format.** Regional offices and institutions use the BP-A1008, Security Technology Evaluation Template when they evaluate a new technology OST believes may be a viable solution to an operational issue (e.g. detecting or combating contraband cell phones). Regions and institutions provide results via a completed template to OST within 30 days of the evaluation's completion. OST provides the results, and its own recommendation, to the Bureau Executive Staff in the appropriate format (BP-A1008, pilot project format, etc.) to better inform Bureau-wide decisions regarding the technology's adoption.

c. **Formal Evaluation or Pilot Testing.** When appropriate, for new equipment being evaluated, OST, the region, division, or requesting institution submits a BP-A1008, Security Technology Evaluation Template or a pilot proposal to the AD, ITDD or the Executive Staff, recommending an operational evaluation or pilot project test, respectively, of the device or equipment at an institution.

Larger pilots may require additional Executive Staff approval before being initiated. See the Program Statement **Pilot Initiatives, Approval and Evaluation**.

Bureau staff report both successful and failed security technologies to OST to help prevent reoccurring expenditures.

## 6. COLLABORATION

Through dissemination of OST formal evaluations, or other technology evaluation and reporting formats, to the NIC or the NIJ, OST enhances agency collaboration with other federal, state, and local organizations.

Through this process, OST documents what is learned and shares throughout the Bureau and, when appropriate, the national professional corrections community, to enhance agency wide knowledge of new security technologies.

## REFERENCES

### *Program Statements*

Pilot Initiatives, Approval and Evaluation

### *Forms*

BP-A1008 Security Technology Evaluation Template

### *ACA Standards*

Performance-Based Standards and Expected Practices for Adult Correctional Institutions (5th Edition): 5-ACI-1F-08, 5-ACI-1F-17

Performance-Based Standards and Expected Practices for Adult Local Detention Facilities (5th Edition): 5-ALDF-7D-20

Standards for the Administration of Correctional Agencies, 2nd Edition: 2-CO-1F-07

### *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.