



**U.S. Department of Justice**  
**Federal Bureau of Prisons**

**PROGRAM STATEMENT**

OPI: IPA/OST  
NUMBER: 1150.06  
DATE: April 5, 2013

## **Office of Security Technology**

/s/

*Approved:* Charles E. Samuels, Jr.  
Director, Federal Bureau of Prisons

### **1. PURPOSE AND SCOPE**

To define the duties and responsibilities of the Office of Security Technology (OST). This office, a branch within the Information, Policy, and Public Affairs Division (IPPA), is responsible for:

- Identifying new security-related technology and equipment.
- Evaluating its potential use.
- Assisting in its implementation.
- Approving any security technology purchase over \$5,000.
- Evaluating its effectiveness.

#### **a. Summary of Changes**

*Policy Rescinded*

P1150.05 Security Technology, Office of (1/29/99)

The Program Statement has been revised to reflect the following:

- Clarifies that OST is not a research and development organization, but conducts operational evaluations of potential technology solutions to Bureau security issues.
- Defines how OST formulates evaluation plans that support a consistent approach to evaluating new security technologies and strengthen agency decisions about deploying them; such plans may include defining measurable objectives and developing a detailed data analysis plan.
- OST technology evaluation plans will clearly define evaluation-related responsibilities for individuals conducting operational test(s) at each institution.

- Requires regions and institutions to provide written operational evaluation results via an OST Technology Evaluation Template (Attachment A; BP-A1008) within 30 days of the evaluation's completion.
- Authorizes 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) to enhance collaboration with other Federal, state, and local organizations.

**b. Program Objectives.** The expected results of this program are:

- 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 field locations.
- 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 on approval of the Assistant Director, IPPA.
- 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.

## 2. RESPONSIBILITIES

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

- a. **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 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 agency use in light of 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 an operational evaluation** for the Executive Staff or appropriate requester that follows the parameters of Attachment A (BP-A1008). When appropriate, the report includes a draft memorandum from the Assistant Director to the field recommending the purchase of the technology and any other relevant product information.

d. **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** 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 reoccurrence.

OST staff are available for onsite review of specific security problems. If a Warden determines that 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 Assistant Director, IPPA. When approved, OST assistance is coordinated with institution staff and Regional and Central Office administrators.

### 4. SECURITY TECHNOLOGY OPERATIONAL EVALUATION PROJECTS

Based upon Assistant Director, IPPA, 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 that support a consistent approach to evaluating new security technologies and strengthen agency 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 that 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 (see Attachment A [BP-A1008]) that can be used in more formal evaluations. Evaluation-related responsibilities are coordinated with institution management to ensure that 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 OST Technology Evaluation Template (Attachment A; BP-A1008). The form must be signed by the Warden, Regional Director, or appropriate Assistant Director and submitted to the Assistant Director, IPPA Division, Attn.: Office of Security Technology.

## 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 OST Technology Evaluation Template, Attachment A (BP-A1008), when they evaluate a new technology that OST believes may be a viable solution to an operational issue (for instance, 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 BOP leadership in the appropriate format (OST evaluation template, pilot project format, etc.) to better inform BOP-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 an OST Technology Evaluation Template or a pilot proposal to the Assistant Director for IPPA 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**.

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

## 6. COLLABORATION

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 enhances agency collaboration with other Federal, state, and local organizations.

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

## REFERENCES

### *Program Statements*

- P1066.04 Pilot Initiatives (11/14/07)
- P4100.04 Bureau of Prisons Acquisitions Policy (5/19/04)
- P4200.10 Facilities Operations Manual (1/24/06)

### *ACA Standards*

- American Correctional Association Standards for Adult Correctional Institutions, 4<sup>th</sup> Edition: 4-4102

- American Correctional Association Standards for Administration of Correctional Agencies, 2<sup>nd</sup> 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 Sallyport.

**Attachment A (available on Sallyport as BP-A1008)**

**OST TECHNOLOGY EVALUATION TEMPLATE**

TITLE OF TECHNOLOGY EVALUATION:

DATE OF SUBMISSION:

ORIGINATING STAFF/LOCATION:

ANTICIPATED START DATE:

ANTICIPATED COMPLETION DATE:

1. State the goals for this evaluation of new security technology.
2. Formally describe your evaluation plan. How will comparisons be made (conditions at similar institutions compared to non-evaluation institutions, conditions before technology deployment compared to conditions after deployment, etc.)?
  - a. Is any baseline data available to use in the comparison? Who will conduct the evaluation?
  - b. Clearly define and articulate the technology evaluation methodology, including sound sampling methods, determination of appropriate sample size for the evaluation design, and a strategy for comparing the evaluation results with other evaluation efforts of this or similar security technologies.
  - c. Delineate how the evaluation plan will obtain the type and source of data necessary to evaluate the technology, methods for data collection, and the timing and frequency of data collection. This detailed data analysis plan will be used to track the technology evaluation's performance and measure the final results of the evaluation.
3. Also, state how evaluation-related responsibilities will be coordinated and approved with institution management to ensure testing duties do not interfere with operational responsibilities of staff members conducting the technology evaluation.
4. List the performance measures (i.e., well-defined, clear, and measurable objectives you will use to assess the success or failure of the technology to meet its objectives).
5. List all criteria or standards for determining the success or failure of this technology evaluation.

a. Criteria to be included is consideration of whether the technology performs within the technical specifications of the manufacturer or governing professional standards (i.e., NIJ, NIST, ASTM, etc.) and whether it meets or fails to meet the stated security objective(s).

b. Standards include evaluating technology against its governing Program Statement if applicable; ACA mandatory or non-mandatory standard, if applicable; agency Use of Force application; and/or Correctional Services Manual, applicable section. List all such directives that were reviewed to design this technology evaluation so that it complies with current agency policy and accepted law enforcement practice.

6. Include a list of subject matter experts (i.e., OST project manager, Correctional Services Administrator, Executive Staff, etc.) who were consulted during the design of this technology evaluation.

7. Discuss any conflicts that may be encountered between this technology evaluation and existing policy. Describe how these conflicts will be resolved.

8. Describe all costs associated with the technology evaluation. If funding is needed, provide cost estimates associated with the technology evaluation; and state how the evaluation will be funded. Alternatively, if the technology evaluation will save money, provide estimated cost savings and explain how these savings will be accomplished.

9. If technology is evaluated, required training will involve (please indicate type of training, number of personnel, and anticipated cost):

10. List relevant concerns and issues in the form of key questions which need to be answered by the end of the technology evaluation.

a. Consider questions such as:

How might the new program positively or adversely impact institution security, public safety, other program areas, staff and inmate morale, and the orderly running of the institution?

b. What positive/negative side effects might occur?

c. What obstacles to this technology's implementation do you anticipate?



11. Approval Signatures:

---

Technology Evaluation Project Manager

---

Chief, Office of Security Technology

---

Sponsoring Warden

---

Sponsoring Regional/Assistant Director

---

Assistant Director  
Information, Policy, and Public Affairs Division