Selection and Application Guide to Offender Tracking Systems
for Criminal Justice Professionals

NIJ Guide 1004.00

Prepared by:
National Institute of Justice
Office of Science and Technology
Washington, DC 20531

June 2012
NCJ xxxxx
The National Institute of Justice is a component of the Office of Justice Programs, which also includes the Bureau of Justice Assistance; the Bureau of Justice Statistics; the Community Capacity Development Office; the Office for Victims of Crime; the Office of Juvenile Justice and Delinquency Prevention; and the Office of Sex Offender Sentencing, Monitoring, Apprehending, Registering, and Tracking (SMART).
Foreword

This document, Selection and Application Guide to Offender Tracking Systems for Criminal Justice Professionals, provides guidance concerning the functionality, procurement, selection, use and maintenance of offender tracking systems (OTSs) used by law enforcement and corrections practitioners to track the location of participants. The primary audience for this guide includes criminal justice officials, departmental and/or governmental technology managers, and system purchasers.

The development of Offender Tracking System Standard (and accompanying documents, including this guide) was undertaken by NIJ to aid criminal justice practitioners in the proper acquisition and application use of OTSs. Documents were developed via a committee approach with the involvement of three groups: a Special Technical Committee (STC), an Advisory Working Group (AWG) and a Steering Committee (SC). Each of these committees supported the development of the documents, ultimately working together to ensure criminal justice community and stakeholder input on this initiative.

This guide broadly outlines the overall functionality of OTSs as operated in the law enforcement and corrections environments, highlighting major system use considerations and stressing the importance of the NIJ Standard. A baseline technical overview of OTS anatomy is presented in order to educate readers on system fundamentals. The guide offers an abbreviated description of the technical standard, written in lay terms so that system purchasers and managerial practitioners can learn why specific components were included. The guide outlines leading practices for system procurement and other supplemental considerations as identified from experience by criminal justice practitioners.

This guide also includes several procurement recommendations – broad enough in scope to be useful to any agency – intended to serve as a resource for system purchasers. The guide also includes a list of participants who took part in development of the documents for the NIJ OTS project.

Nothing in this document is intended to create any legal or procedural rights enforceable against the United States. Moreover, nothing in this document is intended to constitute or imply any endorsement, recommendation or favoring by the United States of any specific commercial product, process or service. Finally, nothing in this document creates any obligation for manufacturers, suppliers, public safety agencies or others to follow or adopt any NIJ voluntary equipment standard.
Contents

EXECUTIVE SUMMARY .................................................................................................................. 1
INTRODUCTION ............................................................................................................................. 3

CHAPTER 1. TECHNOLOGY OVERVIEW ...................................................................................... 5
  ACTIVE, PASSIVE AND HYBRID TRACKING ............................................................................. 5
  MULTI-PIECE AND ONE-PIECE DEVICES .............................................................................. 5
  POST-PROCESSING AND ONBOARD PROCESSING SYSTEMS .............................................. 6
  AUXILIARY EQUIPMENT ........................................................................................................... 7

CHAPTER 2. PROCUREMENT CONSIDERATIONS ...................................................................... 8
  CHOOSING THE PROPER TECHNOLOGY .............................................................................. 9
  VENDOR CONSIDERATIONS ................................................................................................... 11
  MONITORING CENTER SERVICES OFFERED ........................................................................ 12
  TRAINING OFFERED .............................................................................................................. 13
  EQUIPMENT TRIALS ............................................................................................................... 13
  COMMON PROCUREMENT PROCESSES .............................................................................. 15

CHAPTER 3. PROGRAM MANAGEMENT CONSIDERATIONS .................................................... 17
  POLICY CONSIDERATIONS ..................................................................................................... 17
  STAFFING AND WORKLOAD .................................................................................................. 17
  BUDGET PLANNING ............................................................................................................... 18
  RESPONSE PROTOCOLS ........................................................................................................ 21
  TRAINING CONSIDERATIONS ............................................................................................... 22
  MANAGING TRACKING EVIDENCE ..................................................................................... 24
  DATA RETENTION CONSIDERATIONS .................................................................................... 26
  LEGAL CONSIDERATIONS .................................................................................................... 27
  MEDIA RELATIONS ................................................................................................................ 27
  PROTECTING DATA BY CONTROLLING ACCESS TO SOFTWARE ....................................... 29
  MEASURING OFFENDER TRACKING PROGRAM OUTCOMES ............................................ 30

CHAPTER 4. OPERATIONAL CONSIDERATIONS ..................................................................... 31
  MATCHING TECHNOLOGY TO OFFENDER TYPE .................................................................. 31
  ERGONOMIC CONSIDERATIONS .......................................................................................... 32
  INSTALLATION ....................................................................................................................... 33
  PARTICIPANT INITIAL ORIENTATION .................................................................................. 33
  INSPECTION, CARE AND MAINTENANCE ............................................................................ 35
  FACTORS THAT IMPACT LOCATION TRACKING .................................................................. 36
  DATA, MONITORING AND ALERT CENTERS ....................................................................... 38
  INFORMATION AND DATA EXCHANGE ................................................................................ 40
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIRCUMVENTION CONSIDERATIONS</td>
<td>41</td>
</tr>
<tr>
<td>CRIME SCENE CORRELATION</td>
<td>43</td>
</tr>
<tr>
<td>REPORT CONSIDERATIONS</td>
<td>44</td>
</tr>
<tr>
<td>BATTERY CONSIDERATIONS</td>
<td>45</td>
</tr>
<tr>
<td>ROBUSTNESS CONSIDERATIONS</td>
<td>46</td>
</tr>
<tr>
<td>COMMUNICATION WITH THE PARTICIPANT</td>
<td>46</td>
</tr>
<tr>
<td>APPENDIX A: COMMON TERMS FOR OFFENDER TRACKING SYSTEMS</td>
<td>48</td>
</tr>
<tr>
<td>APPENDIX B: LINKS AND REFERENCE MATERIALS</td>
<td>58</td>
</tr>
<tr>
<td>APPENDIX C: OFFENDER TRACKING SYSTEM PROJECT ROSTERS</td>
<td>60</td>
</tr>
</tbody>
</table>
Executive Summary

Offender tracking system (OTS) technology has emerged as an important tool for an agency’s mission of managing selected participants in the community. Whether an agency faces a mandate to track sex offenders, has a need to more closely monitor higher risk offenders or is looking for confinement alternatives for low-risk offenders, this technology can often be a helpful tool. However, misunderstanding the technology’s limitations can lead to unrealistic expectations. Also, selection of a system that does not best meet an agency’s needs can result in frustrated workers and criminal justice partners, disgruntled supervisors and a community unsatisfied with the level of public safety provided.

Selection and Application Guide to Offender Tracking Systems for Criminal Justice Professionals (hereafter, the guide) offers agencies assistance on a variety of OTS issues. The information provided herein will create a better understanding of the technology while offering proven strategies for managing a program. In addition to providing an overview of the technology, this guide addresses three broad topics: procurement considerations, program management and operational issues.

When choosing an OTS vendor, your agency should select the most appropriate technology for the intended population. Procurement officials need to consider a number of hardware and software issues. You should have a thorough understanding of a bidder’s proposed technology and take the equipment on trial, if possible. Consider feedback from supervising officers before making a final selection. Investigate the credibility of the vendor, including the steps taken to maintain the integrity and security of the data.

The management of an OTS program can be complex and requires quite a different skill set from that needed to oversee a traditional community supervision program. Prepare policies that clearly define all aspects of the program’s objectives and delineate who is responsible for each activity. Officers need specialized training to master the highly technical aspects of the program. Agencies need to teach officers how to manage evidence relating to participant tracking violations as well as prepare them to address tracking technology competently in a court of law.

As a manager, you should be able to obtain sufficient funding for an OTS program. Agencies often underestimate officer workloads associated with OTS programs, resulting in inadequate budgets. Ensure that the program’s data is protected by assigning levels of access to appropriate staff while taking steps to prevent hackers from also gaining access. Prepare to address media issues, especially when a high-profile event occurs. Finally, you should monitor measure the...
success of a program by measuring performance outcomes and comparing them with the program’s objectives.

All officers involved in the program need to understand a number of operational features of OTS technology. They should know the most secure method of installing a tracking device on a participant, how to protect the security of inventoried items and how to properly care for the equipment.

Your agency should teach participants acceptable cleaning methods and provide an orientation to the participant that will encourage schedule compliance.

When evaluating tracking points, you must be able to understand all of the factors that impact accuracy before making a decision that a violation has occurred. You should know how to generate the reports needed for the day-to-day supervision of a caseload while understanding the process required for obtaining special reports, and understand the conditions under which an OTS device is intended to operate. Factors such as extreme temperatures, high humidity and shock can have an adverse effect on tracking equipment.

This guide provides a glossary of terms commonly used in the OTS industry in an appendix. There has been much confusion over terminology and this glossary should serve to provide clarity. The guide provides references to publications and links to websites for additional resources on these topics. It also includes a listing of the members of the Special Technical Committee that worked on the Offender Tracking Standard.
Introduction

History
In 1996, participants began carrying the very first tracking devices in bulky backpacks. Conceptually, they were the same as many of the multi-piece devices on the market today. Each consisted of a cell phone, a GPS receiver and a battery integrated into a box weighing several pounds. The device was electronically tethered to the participant with a transmitter attached to the ankle. Although the GPS chipsets used were primitive by today’s standards, and the cell phone rapidly drained the battery, the system was considered a breakthrough and it launched a new era for the criminal justice system.

In the late 1990s, there were just two manufacturers of OTS equipment; today, the industry includes more than a dozen companies. For the most part, this is great news for agencies. Not only has the competition driven prices down, but agencies are now more likely to find products with features that will better meet their specific needs. New features offered include voice communication, audible and vibratory alerts to warn participants of schedule violations, improved software for user-friendly case management, superior mapping technology with playback capabilities and mobile restriction zones that can be used to keep a participant away from other tracked participants, just to mention a few. As the use of this equipment increases, more innovations can be expected and leasing costs for the equipment may decrease even further.

Need for a Standard
Unfortunately, all of this market growth and product innovation has occurred in an environment where there are no standards in place. This has resulted in end user confusion about the capabilities of the products they have procured. As a result, unrealistic expectations for OTS programs and disgruntled stakeholders are commonplace. The Special Technical Committee (STC) found a lack of consensus among its members over the meaning of even the most basic concepts of offender tracking, including active tracking, passive tracking, accuracy and battery life. Without clear definitions for these terms, it is impossible for agencies to compare the relative value of one product to another.

Members of the National Institute of Justice (NIJ) Community Corrections Technology Working Group (TWG) have been hearing concerns from the criminal justice community about these issues for many years. In 2006, the TWG decided to make the development of a standard for OTS technology one of its top priorities. NIJ found funding for the project in 2009 and
established the Offender Tracking Standard STC to develop such a standard. The first meeting of
the Offender Tracking Standard STC took place in September 2009.

Much of the demand for OTS products has come about as a result of legislative mandates. By
2010, 33 states had enacted legislation requiring that this technology be used on sex offenders.
However, many of these states have not yet implemented the programs, and several others have
newly formed programs. Considering there are more than 625,000 registered sex offenders in the
United States, there appears to be plenty of room for continued growth in the use of offender
tracking technology. Some states have begun using OTS technology to track gang members and
other jurisdictions use the devices to monitor habitual burglars, track domestic abusers and alert
victims. It is reasonable to expect many other applications for this technology in the criminal
justice field in the future.

The demand for OTS technology is great, and the products are becoming more innovative and
affordable. However, without the presence of a standard that delineates performance
requirements, it is difficult for an agency and its procurement officers to know whether the
equipment they are procuring will fully meet their needs. The goals of developing the Offender
Tracking Standard and the associated conformity testing program included clearly setting forth
the definition of terms, confirming equipment performance claims under realistic and controlled
environments, and ensuring that the devices are robustly built and less vulnerable to
circumvention attempts.
Manufacturers of OTS equipment use a variety of technologies and equipment configurations to monitor and record the location of participants. It is important for your agency to understand how the systems function so it can make an informed decision when selecting an OTS technology.

**Active, Passive and Hybrid Tracking**

*Active* systems are usually capable of collecting location points at a rate of at least one point per minute. An active system provides location and status information to the agency in near-real time. An agency also can request updated location information (“ping a device”) and receive near-real time location and status data from an actively reporting device.

A *passive* system works similarly to an active system, except location and status information is uploaded to the data center at predetermined intervals, usually once per day. A passive device usually cannot be pinged for current location and status data.

*Hybrid* systems are not addressed in the standard, but are commonly mentioned by OTS vendors. Although no universally accepted definition or functionality exists for a hybrid system, the general consensus is that a hybrid system operates in a passive mode until any of several predetermined triggering events occur, causing the device to switch to an active reporting mode. Common triggering events include zone infractions, tamper indications and low power status.

**Multi-Piece and One-Piece Devices**

Agencies contemplating an OTS program face an important question: should they select a one-piece or a multi-piece tracking system? Both types of systems have advantages. Your agency’s objectives should play a large part in deciding which type of device will work best for its needs.

A one-piece device has many benefits. One-piece devices require fewer pieces of equipment in inventory and less storage space. They remove the need to tether the tracking unit to another device to ensure the equipment is with the participant. “Bracelet Gone” alarms sometimes overwhelm an agency’s staff and use of a one-piece device eliminates such alarms. Also, participants need not remember to carry an unattached tracking device with them at all times – a requirement with which some cannot (or do not) consistently comply.

On the other hand, multi-piece systems can offer more security than most one-piece devices. Multi-piece systems equipped with motion sensing technology can tell whether the tracking unit is at rest. This information is important when a participant enters a heavily shielded indoor structure and tracking is interrupted. If the device is at rest and the participant is in range of the
device, the participant’s location can be established with a high degree of certainty. Because most participants spend a majority of their time indoors, this is no small issue. One-piece devices cannot easily capitalize on this technology; even when sleeping, a participant’s leg moves frequently and therefore the device is never completely at rest.

Most one-piece tracking devices rely on cellular communications and thus are of little value in areas where there is no cellular coverage. For example, a number of participants live in remote geographic areas of the country. Due to a lack of cellular coverage, many of these participants can only be tracked passively with devices that have a landline option for uploading data.

Signal reception is typically better with a device worn at waist level. Generally, the higher the tracking device is above the ground, the better the reception will be. One-piece devices worn at the ankle are also more frequently subjected to unintentional shielding. For example, when a participant drives a vehicle, the ankle-worn device is usually under the dashboard and only a short distance from the engine block, not an advantageous place for radio frequency (RF) reception and transmissions to occur.

**Post-Processing and Onboard Processing Systems**

An often overlooked design consideration is how OTSs process location and schedule events. Where a system stores its zone and schedule information can have a significant effect on how quickly and efficiently an agency receives notice of noncompliance. Zones and schedules can be stored either on the tracking device or on a server in the vendor’s data center. In some cases, the system stores the zones in one location and the schedules at the other.

Systems that use *post-processing* of collected location data store the participant’s zone and schedule information at the data center. After the tracking device uploads location data, the information is compared to the participant’s inclusion zones, exclusion zones and schedule. Any detected noncompliance results in notification to the supervising agency. Strictly enforcing zones and schedules of participants of post-processing systems requires frequent uploads of location data.

*Onboard processing* systems store zone and/or schedule information on the tracking device assigned to the participant. With this configuration, the participant’s location can be immediately compared to his/her inclusion zones, exclusion zones and/or schedules in order to more quickly identify infractions. An infraction will trigger an immediate upload to the data center and agency notification. With onboard processing, your agency can schedule less frequent uploads (during periods without infractions), which saves in communication costs while conserving power.
Intellectual property rights may limit where a vendor stores zones and schedules. However, the need for agencies to quickly identify program noncompliance without increasing costs is driving the market to create new and innovative ways to efficiently provide agencies with timely alerts. An agency should discuss the methodology used with any potential vendor before selecting an OTS.

**Auxiliary Equipment**

*Beacons* are optional cordless RF transmitting devices designed to work in conjunction with both one- and multi-piece OTSs. Some beacons switch the location system to an RF mode when the tracking device comes within a designated range. Beacons also allow agencies to track when a participant enters or exits a designated area. An agency places a beacon at a known location, usually the participant’s home or workplace. When a tracking device comes in proximity to a beacon, it can turn off other location technologies. This can significantly increase the interval between battery charges. It also enhances accuracy by eliminating occasional inaccurate location points obtained from GPS or other location-based systems. Your agency should know the distance at which a beacon will operate and if you can adjust that distance.

*Car chargers* are useful auxiliary equipment for participants who do not always have ready access to an alternating current (AC) power source, but agencies should caution participants about charging while driving. Some agencies supply participants with car chargers to use in the event of a power failure caused by natural disasters. Car chargers are also helpful for participants who travel long distances, such as truck drivers, and for homeless participants who live in their cars.
Chapter 2. Procurement Considerations

Criminal justice agencies are becoming more involved in the use of technology as a means to track and monitor participants. New laws and public demands task these agencies with maintaining public safety while monitoring higher risk participants in the community. Your agency should evaluate a number of factors prior to making a procurement decision. This chapter discusses these factors in detail.

Importance of Certification

Purchasing agents should procure only certified products (those deemed compliant with the requirements of NIJ Standard 1004.00 as determined by an independent, third-party certification body). This certification gives the end user a level of confidence in the performance of the OTS. The certified product will include the certification organization’s mark of conformity in addition to, or attached to, the product label to demonstrate compliance with NIJ Standard-1004.00. When procuring certified equipment, purchasing agents should confirm the presence of the certification organization’s mark. NIJ CR-1004.00 specifies requirements for the independent third-party certification of OTS equipment.

Some key items addressed within NIJ CR-1004.00 include:

- Initial evaluation and testing according to the requirements of the standard and a review of documentation needed prior to production of the OTS model.
- Bi-annual evaluation to include an onsite audit of the manufacturing location(s). The audit shall include, at a minimum, a review of the OTS manufacturer’s quality management system. The certification organization will evaluate the product and make a determination on testing that may be required.
- Actions to be taken in the event of hardware or software changes. If a manufacturer chooses to make a system-level hardware component change or proposes to alter the methodology used for determining location, the OTS manufacturer shall submit that change and related documentation to the certification organization prior to implementation. The certification organization will determine (1) which tests, if any, are required to be performed to demonstrate continued compliance and (2) whether the change is so significant that it will result in a new model.

The benefits of procuring and using certified systems include:
The standard and conformity assessment documentation were developed by practitioners to address the needs of the field, and take into account operational requirements.

OTS models are tested and certified by independent organizations.

Certified OTS models are listed on publicly accessible certified products lists (CPLs).

An informational page for OTS models is available on http://www.justnet.org and includes the NIJ documents and links to CPLs. This page is a “one-stop” Internet resource containing relevant details and links for agency managers, procurement officials and end users.

The availability of certified models listed on an Internet-based CPL means that it is not necessary to rely solely on manufacturer claims.

Choosing the Proper Technology

There are a variety of tracking technologies used to monitor participants’ locations. (See Active, Passive and Hybrid Tracking; Multi-piece and One-piece Systems, and Post-Processing and Onboard Processing in Chapter 1.) Choose the technology that best meets your agency’s objectives. Whether your agency chooses active or passive tracking may depend on the risk level of the participant and/or expected response time to alerts. Whether the technology will alert a victim to the proximity of a participant also can play an important role in technology selection. Some agencies may have a preference for either one-piece or multi-piece systems.

Because not all vendors offer each of these configurations, your agency may narrow the list of potential vendors by deciding on a technology. However, before prematurely eliminating a type of technology, you should thoroughly evaluate each approach and weigh each against program objectives.

Hardware Considerations. In addition to the factors discussed in Chapter 1, your agency should also ask other questions about the proposed hardware. They include:

- Is the size and weight of the device acceptable for its intended application?
- Does the device use multiple location technologies?
- What is the expected battery life between charges under normal use?
- What is the manufacturer’s suggested charging time?
- How many times can a battery be charged before it needs to be replaced?
• What cellular provider does the vendor use for active tracking? Is that cellular provider the best choice for the locations where the participants will be tracked?
• Can the vendor use more than one cellular provider?
• Does the vendor offer accessories such as car chargers and beacons?
• Does the device have the ability to monitor in both active and passive modes?
• Does the device use any motion-sensing technology that can extend battery life?
• Is the device designed with tamper-evident features?
• What, if any, device components are considered consumables?

Software Considerations. Software features and usability may be the most significant factors in determining your agency’s overall satisfaction with its selected OTS. Your agency should carefully consider a bidder’s software features. Be sure to ask the following:

• Is the software web-based?
• What are the minimum requirements for the agency computers?
• Does additional software need to be added to agency computers?
• Is mapping of the jurisdiction up to date? Are new housing developments and roadways displayed in the vendor’s mapping?
• Are aerial and street views available?
• Does the mapping software display points of interest?
• Can the mapping software perform reverse geocoding?
• Does the software allow for the creation of free-form zones?
• Can global zones be developed?
• Can zone templates be created for certain classes of participants?
• Are the reports generated by the software consistent with the needs of the agency?
• Can the vendor provide custom reports as needed?
• Can the system perform automated crime scene correlation (instantly querying all participants about their presence at a designated location at a designated time)?
• Can the software notify officers in the field of alerts?
• Is the software accessible via portable mobile devices such as smart phones and tablets?
• Can the OTS data be easily integrated with an agency’s case management system?

After gathering information about the bidder’s hardware and software, ask vendors for a free trial of their tracking system (see Equipment Trials later in this chapter). Validate their responses and have users evaluate system functionality. (For additional information about selecting the appropriate technology, please refer to Matching Technology to Offender Type in Chapter 4.)

Vendor Considerations

Selecting the right vendor is critical to the success of an OTS program. When evaluating and selecting a vendor, your agency should consider many factors, most of which should be addressed during the procurement and contract process. Agencies also should evaluate the technical support and training provided by the vendor.

Below is a list of other questions an agency should ask a potential vendor:

• How many years has the vendor been in business?
• Will the vendor disclose its corporate financial records, including profit and loss statements for past five years?
• What types of technologies are offered?
• How many of the vendor’s OTS devices are currently in use?
• Do the vendor’s current and past customers provide positive references?
• Will the vendor disclose current and previous legal actions in which it was named as a plaintiff or respondent? If applicable, what are the statuses/outcomes of these cases?
• Does the vendor have a quality assurance/quality control program in place for its systems, equipment and services?
• Does the vendor have a staffing plan? How does the vendor determine if there is sufficient staff to service its customer base?
• Does the vendor have employees who can competently attest to its methodology and products’ performance in any legal proceedings?
• How will equipment returns be handled and at whose expense?
• Will the vendor allow a percentage of spare tracking devices at no additional cost?
• Who will be responsible for lost or damaged equipment?
• Will the vendor supply updated equipment when it becomes available?
• Does the vendor provide field support?
• Does the vendor have written policies and procedures in place for its employees?
• Is the vendor a manufacturer or a third-party vendor?

Monitoring Center Services Offered

When evaluating a vendor, your agency should consider the type of support services needed to effectively manage the monitoring program. A vendor can offer various levels of support. Some agencies prefer a full-service option that provides onsite vendor representatives who install equipment and respond to all alerts. Other agencies choose to do all of the work themselves and rely on the vendor to provide only automated alerts.

These varying levels of support may be offered at significantly different costs. Your agency should choose a plan that best meets the needs of the program while staying within budget restrictions.

For vendor-operated monitoring centers, your agency should consider the following factors:

• What level of service is the vendor proposing and at what cost?
• During what hours of operation is the service available?
• Are there sufficient phone lines to accommodate anticipated communication needs and sufficient support staff to handle issues as they arise?
• Does the vendor have the ability to implement custom alert notification protocols for the agency?
• Does the vendor conduct criminal history checks of monitoring center employees and provide that information to the agency?
• Does the vendor maintain a secure offsite facility for storing backup data?
• Are there redundant sources of communication and power?
• Has the vendor previously lost any agency’s historical data?

For additional information on monitoring centers, please refer to Data, Monitoring and Alert Centers in Chapter 4.
Training Offered

A critical requirement for a successful OTS program is a high level of staff proficiency with the technology. Although in-house trainers can be helpful, most agencies rely on the vendor to provide comprehensive initial and follow-up training. Questions about vendor-offered training should include:

- Does the vendor provide onsite training for agency staff at no extra cost?
- What is the length of the initial training?
- Will the vendor co-present with an agency trainer to ensure that the training addresses specific program needs?
- Does the vendor provide troubleshooting and follow-up training as needed by the agency?
- Does the vendor provide current operation manuals to the agency?
- Does the vendor provide a training curriculum for agency staff?

For additional information on training, please refer to Training Considerations in Chapter 3.

Equipment Trials

All vendors should allow an agency to test equipment prior to making a final procurement decision. Many factors can only be evaluated during a free trial period.

**Cellular Coverage.** All active OTS devices, and some passive systems, contain cellular technology. Vendors choose one or more cellular provider(s) to provide location and status data from the tracking device to the data center. Your agency should know if the vendor’s cellular service provider has limited or no coverage within portions of your jurisdiction. During a trial, your agency should check for cellular operability in all areas where participants may be allowed to spend time.

**Accuracy.** A number of factors can impact accuracy. In fact, it is virtually impossible to totally control all of the variables affecting accuracy outside of a laboratory setting. The standard requires OTSSs to undergo stringent testing in controlled environments, both indoors and outdoors. However, your agency can take a few simple steps to help you understand how accurate tracking devices can be in various environments. Because you cannot control for all variables, results should be interpreted accordingly.
By evaluating several tracking systems simultaneously, an agency can evaluate the relative accuracy of each one. Testing for accuracy in this manner technically does not control the variables, but it does subject each of them to the same environment at the same time. If an agency has only one tracking device to evaluate at a time, a fair comparison of accuracy may be more difficult to achieve.

Conduct accuracy trials in the following locations:

- In an open field, place the device(s) in a location easily identifiable in an aerial/satellite view provided through the vendor’s mapping software. Such locations can be the pitcher’s mound of a baseball park or the 50-yard line of a football field. You can easily compare the plotted locations to the actual locations used during testing.

- Place the device(s) near a large body of water (if applicable) for an extended period (12 hours or more) to determine the degree of multi-path error that occurs. RF signals tend to skip over some water surfaces much like a stone. You may find that tracking devices that accept satellite signals approaching from near the horizon report location points with greater accuracy error than those that do not.

- Take the device(s) along a predetermined route in an urban canyon (if applicable) where a cluster of high-rise structures significantly blocks the view of the sky and limits the number of satellites in view.

- Take the device(s) along a predetermined route in a wooded area where foliage blocks the view of the sky and limits the number of satellites in view.

- In a residential setting, place the device(s) in the center of a typical house to see how the local construction material impacts the reception of location signals.

- Take the device(s) into a large office building or shopping mall where there is limited access to windows or skylights.

(For additional information on Accuracy, see Factors That Impact Location Accuracy in Chapter 4.)

**Battery Life Between Charges.** When performing accuracy tests, keep a record of how quickly the battery discharges. Under typical conditions, a tracking device should maintain sufficient power to track throughout a participant’s daily routine. Keep in mind that new batteries tend to have a longer life than older batteries; this will become a factor when your equipment begins to age. The testing also should measure the time required to completely recharge a fully discharged battery. One-piece tracking devices attached to a participant should fully recharge in two hours.
or less. Any charging time longer than this likely will result in more frequent low battery alerts as participants may not be willing to remain stationary near an electrical outlet for that long. Multi-piece systems equipped with a charging stand for the tracking device may have a slight advantage, as they can be charged while the participant sleeps. (Charging while sleeping is not recommended for one-piece tracking devices.)

The standard has stringent requirements on battery life. All one-piece, body-attached devices tested for compliance with the standard are limited to total charging times of two hours per day. Multi-piece configurations can pass the standard with charging periods of no more than four hours each day. (Multi-piece devices are allowed to charge longer because they are typically not worn while being charged.) The objective is to make it more likely that approved systems will provide a full day of monitoring with reasonable charging times. An agency that creates numerous zones (resulting in more alert states) or activates optional energy-expending, vendor-added features may find that the time between charges needs to be shortened.

Common Procurement Processes

Invitation to Bid (ITB). An ITB is a written solicitation for competitive sealed bids. An agency uses an ITB when it can specifically define the scope of work for which a contractual service is required or when it can establish precise specifications that define the actual commodity, or group of commodities, required. An agency reviews a bid strictly against the General Terms, Special Conditions and Specifications of the ITB, and makes an award to the bidder that meets the bid requirements and offers the lowest cost to the agency. Because of the complexity of an OTS, your agency might find it challenging to use the ITB process.

Request for Proposals (RFP). An RFP is a written solicitation for competitive sealed proposals. An agency uses an RFP when it is not practical to specifically define the scope of work for which the commodity, group of commodities or contractual service is required, and when the agency requests that an interested vendor propose a commodity, group of commodities or contractual service to meet the specifications of the solicitation document. An RFP allows for numerous methods by which a project result can be achieved. Price is not the primary factor in evaluation.

An RFP seeks the best value through the competitive bid process, yet provides for both objective and justifiable reasons for choices made. The RFP describes in detail the project to be completed, the intended result and the criteria for choosing a successful bid. It can propose a preferred method of completing the work or can ask the proponents to provide solutions, seeking the creative input of suppliers. The RFP can be as simple or as detailed as needed, allowing greater flexibility in its design, yet must be evaluated according to the published criteria for evaluation.
You should use an RFP when your agency knows **what** is wanted, **when** it is wanted and **why** it is wanted, but not necessarily **how** to meet the need.

Each proposal is evaluated against each of the other RFP responses using a point system, with points given each proposal by an evaluation team. Your agency makes an award to the highest-ranking proposal.

**Invitation to Negotiate (ITN).** An ITN is a written solicitation for competitive sealed replies to select one or more vendors with which to commence negotiations for the procurement of commodities or contractual services. An agency uses an ITN when it determines that negotiations may be necessary to receive the best value. The ITN process brings together vendors that may be capable of providing the required commodities/contractual services. If one or more of the following criteria apply, an ITN is probably the most applicable purchasing method:

- The scope of work for the contract cannot be accurately and completely defined. This often occurs with acquisitions of rapidly changing technology, outsourcing or complex services.
- The commodities/contractual services can be provided in several different ways, any of which would be acceptable. This often occurs with acquisition of emerging technologies or complex services.
- Contractor qualifications and the quality of the commodities/contractual services to be delivered can be considered more important than the contract price.
- The possibility that responses may contain innovative solutions that differ from what was requested. The ITN process allows your agency to consider those types of alternatives.

Your agency will find example procurement documents on the Electronic Monitoring Resource Center website ([https://emresourcecenter.nlectc.du.edu](https://emresourcecenter.nlectc.du.edu)).

--

*June 2012: Draft for Public Comment*
Chapter 3. Program Management Considerations

Your agency should know about the numerous program management issues that can impact the success of an OTS program. This section identifies these topics and provides a general understanding of how they can affect a program.

Policy Considerations

OTS program policies and procedures outline the relationship between an agency’s vision and its day-to-day operations. Policies and procedures allow management to steer OTS program operations without continuous intervention. A well-written policy allows employees to understand their roles and responsibilities within their agency. Offender tracking policies identify the most important actions necessary and provide a general strategy to decision-makers on how to address concerns as they occur. Sound policies and procedures will help your agency reach its program goals.

As your agency develops policies and procedures, it should take care to:

- Provide a clear and concise delineation of the program’s objective.
- Refer to case law, enabling legislation and/or any regulations that impact the program.
- Clearly define responsibilities at all levels.
- Define key term definitions to establish a common language.
- Determine appropriate measures of effectiveness that will quantify outcomes.
- Provide references to documents that relate to the policy.
- Maintain a detailed list of revisions to track edit history.
- Include all program forms to ensure uniformity and proper record keeping.
- Maintain documentation in a secure electronic format.

Staffing and Workload

Agencies should consider the impact that tracking will have on workload. Agencies that are adding offender tracking technologies to augment their other supervision strategies must recognize that implementation can significantly increase staff workload. The decisions you make about the size and objectives of a tracking initiative will have long-range effects on workload. A successful program will have sufficient staffing in place to meet the increased workload demands.
Consider agency and stakeholder expectations and, if necessary, clarify them. The technology selection will impact staff time and expectations regarding the level of response to notifications of potential violations. How your agency implements OTS technology can impact the distribution of the office’s workload. Some agencies may experience workload efficiencies with specialization, while others may not have a large enough population to support specialization.

The tracking technology chosen, along with the expected level of response to notifications, may have a significant impact on workload. For example, probation and parole agencies traditionally operate during normal business hours on weekdays. If your agency expects officers to respond to violations immediately, it will need to develop strategies for 24/7 response. In addition, agencies should consult with legal counsel to determine the implications of their response strategy and to mitigate liability issues. Some agencies believe choosing passive tracking technology that notifies staff of alerts and tracking violations only during scheduled working hours provides the answer to avoiding these workload issues. Although this approach may reduce the amount of after-hours work, there is no evidence that passive tracking reduces the total number of alerts that require attention (see Personnel Costs in the next section).

Many agencies require supervising officers to meticulously review the tracking points of participants under their supervision on a daily basis. By doing this, officers can learn participants’ movement patterns and look for variations in these patterns that merit follow-up investigation. However, this analysis may require many hours of tedious work each day. Software developers are working on methods to automate this process, but until such products become available, an agency should expect that a requirement to review offenders’ tracks daily will require a substantial number of work hours.

As noted in other sections of this document, OTS involves multiple new duties (e.g., participant orientation, participant enrollment, installation of hardware, inventory management, responding to notifications). Assigning these duties is also part of the implementation and will impact workload. Some agencies opt to do everything in-house, whereas others may contract out all or part of the work. The duties an agency decides to keep impact staff workload. Also, even if a vendor or other outside entity completes duties, agency staff still need time to communicate with the external entity regarding ongoing operational issues as well as unique situations that arise.

**Budget Planning**

Perhaps the most common problem cited by OTS program administrators is lack of a sufficient budget to properly operate their programs. Many costs associated with running a program are underestimated or entirely overlooked. By recognizing the cost categories, agencies can better
understand the anticipated costs of a program and take steps to obtain adequate funding prior to initiation.

This section discusses four major categories of cost:

- Tracking equipment.
- Personnel costs.
- Administrative expenses.
- Support equipment.

**Tracking Equipment.** Of the expense categories, this one is the best understood and accounted for by budget planners. A bid resulting from an RFP or ITB should clearly delineate the proposed costs to an agency for the lease or purchase of tracking equipment. However, oversights can be problematic.

In most cases, agencies choose to lease tracking devices. Because the technology is rapidly evolving, purchase of devices may leave an agency with obsolete equipment after just a few years. Provisions of a lease should include language that allows the agency to receive newer models as they become available.

The equipment assigned to participants often requires maintenance. When an agency purchases equipment, it usually assumes responsibility for the cost of repairs. A carefully worded lease can shift this expense to the manufacturer.

Some leases also have provisions for the manufacturer to replace lost or stolen equipment. Such contracts may have a higher daily lease rate, but agencies have the assurance they can continuously monitor a specific number of participants at a known monthly cost. If an agency purchases equipment, the number of participants an agency can supervise will steadily decrease as devices become inoperable, lost or stolen. The same can be true for agencies that enter into lease arrangements that do not adequately address this issue.

**Personnel Costs.** Agencies commonly assume existing staff can take on the added responsibilities of a tracking program. As discussed earlier in this chapter, tracking programs are very labor-intensive and almost always require a significant investment in added staff time. An active tracking program produces alerts that require 24/7 response. Traditionally staffed agencies that attempt to operate an active tracking program sometimes conclude they cannot handle the volume of alerts that occur after working hours and during the weekends. Without adding staff,
such agencies usually experience officer burnout, unanticipated overtime expenses, high turnover rates and protests from collective bargaining groups.

Other agencies choose to use OTS technology in a passive manner. Rather than receiving alerts 24/7, agencies receive a summary of a day’s activity at the beginning of the next business day. By using this approach, some administrators feel they do not need to increase staffing. This is flawed thinking, because the system generates the same number of alerts as does an active program. It is true that officers assigned passive caseloads will not spend as much time in the field responding to real-time events; however, this does not mean less work. Officers still must take appropriate action, even if it occurs at a later time.

Some agencies, by policy, require officers to conduct a daily review of individual participant tracking points. These agencies must understand that this activity is highly labor intensive and has resource implications regardless of whether active or passive OTS technology is used.

Many agencies use alert centers to reduce the personnel costs associated with a properly run OTS program. These centers are often staffed 24/7 and are designed to triage alerts before center staff pass them along to supervising officers. Participants often forget to charge their devices or they arrive home a little late for a curfew. Alert centers can easily address these minor program breaches by calling participants and reminding them of their program obligations. Agencies can contract for alert center services or may choose to develop their own in-house. Either way, this can be an effective strategy for keeping the personnel costs of an OTS program in check.

**Administrative Expenses.** In addition to line staff, OTS programs require administrative support. This may include clerical assistance, supervisors and program administrators. Typically, an agency needs one supervisor and one clerical assistant for every five to seven supervising officers. Larger programs with numerous supervisors should also plan on budgeting for a program manager to run the tracking program.

Because of the time spent on procurement needs, human resource requirements, policy development (and revisions), auditing and staff evaluations, your agency may need to add an additional five percent to the overall OTS program budget to address miscellaneous administrative expenses. Your agency may find it difficult to identify these expenses when planning a budget, but they most certainly exist.

**Support Equipment.** Officers who supervise monitored participants need to be properly equipped to perform their duties. Because much of their time may be spent in the field
supervising higher risk participants, your agency should make giving these employees adequate safety equipment a priority. It should also budget for office equipment and supplies.

Response Protocols
OTS software typically operates on an exception basis. This means that during setup, agencies define specific parameters for such things as participant curfew, schedule, and inclusion and exclusion zones. When a participant violates those parameters, the software generates an alert to which someone must respond.

When your agency develops OTS program response protocols, answer the following questions.

- Will the agency monitor alert notifications 24/7 or only during normal business hours?
- Will the agency implement its own alert center to handle alert notifications or use the vendor’s monitoring center to assist with this process?
- Will any monitoring center alert intervention occur? Many vendor monitoring centers will act as a first line of defense in an attempt to resolve alert notifications based on agency protocols. This can significantly reduce the number of alert notifications handled by agency staff. If the agency decides to run its own 24/7 operation, it will need to identify on-call staff for monitoring after-hours alert notifications.

Also, consider:

- The costs and increased workload on staff associated with developing 24/7 alert response protocols.
- Union/bargaining agreement issues associated with overtime and on-call hours.
- When a participant can be notified of violations via vibration or sound, implementation of a grace period or delayed agency notification to allow the participant to correct his/her behavior can help reduce administrative/nuisance alerts.
- Clearly defining all individual alert notifications and specific officer responsibilities related to each alert, including proper documentation of how each alert is resolved.
- Victim participation and notifications.

The next section gives two examples of common alert notifications and sample response protocols to demonstrate how a response protocol can be structured.
• *Inclusion/Home Zone* refers to a geographic area within which the participant must stay during a predetermined period of time (e.g., home or work location). When an alert is generated, an agency should:

  o Check the participant's approved schedule and zone to verify for accuracy.
  o Contact the monitoring center to determine the status of the participant alert notification and whether it has cleared.
  o Check to see if the participant lost the GPS signal before returning home and failed to reacquire it.
  o Contact the participant to troubleshoot the problem. This contact will be via verbal conversation over the telephone or may require a field visit with the participant if unable to establish phone contact.
  o Instruct the participant to go outside with the tracking device to re-acquire GPS if the “Home Alert” is a result of losing the GPS signal.
  o Question the participant on her/his whereabouts and the reason for the tracking system’s reflecting an unauthorized absence or being out of place without prior permission from the officer (if GPS was not lost).

• *Device Low Battery*: The tracking device battery needs to be charged to avoid shutdown.

  o Determine the status of the participant alert notification and whether it has cleared.
  o Contact the participant to question his/her activities leading up to the alert. This contact may be via verbal conversation over the telephone or may require a field visit with the participant if unable to establish phone contact.
  o If the previous charge time was sufficient, replace the device and/or charging unit.
  o Instruct the participant to charge the device as soon as possible.
  o Review the participant’s daily charging history to determine previous length of charge and if it was performed according to the manufacturer’s specifications.

**Training Considerations**

As with implementing any other new technology or process, effective training is critical. OTS vendors often offer agencies one to two days of equipment and software training as part of their lease obligation. Agencies sometimes offer additional in-house training to supplement the
vendor’s training. Most agencies offer refresher training at least once a year, conducted either by
the vendor or by an agency staff member who has extensive knowledge of the OTS program and
agency policy. You do not necessarily have to conduct these training sessions through face-to-
face meetings; consider alternative platforms such as live online meetings or on-demand video.

Staff monitoring participants with OTS need a fundamental understanding of the technology as
well as a basic familiarity with computers. This training should also include the strengths and
limitations of the technology. Additional specific training regarding the chosen hardware is
critical. Although there are similarities in hardware offered by different vendors, there can be
significant differences. Monitoring staff need to be very familiar with the selected hardware,
including its installation and how to detect signs of tamper. Similarly, each vendor’s user
interface is unique: monitoring staff need to understand the software capabilities and
navigational tools unique to the chosen vendor’s software.

For some agencies, training on the hardware and software is part of the contract with the vendor.
However, knowledgeable agency staff should also be present. Agency-specific information helps
set expectations and achieves integration with supervision. Staff new to OTS technology can ask
questions specific to their daily duties.

Your agency needs to provide new staff members with proper training. Depending on the level of
training required by agency policy, the length of the program can range from one week to several
months. All new hires should learn the fundamentals of OTS technology, its uses and its
limitations. Staff should fully understand the specific vendor’s equipment and software before
receiving a caseload.

Finally, your agency should recognize that staff require ongoing training due to turnover,
enhancements to hardware and software, and the simple need for a skills refresher. Whether this
ongoing training is offered by recorded media, through an interactive computerized format or
presented live, it can serve to institutionalize standard practices and help your agency achieve
satisfaction. Commonly, staff training should:

- Make it clear that OTS is a tool to enhance staff’s ability to better monitor and more
effectively supervise participants, and is not intended to be a panacea.
- Attempt to dispel any preconceived notions of unrealistic performance.
- Provide training manuals and vendor materials for reference.
- Make sure officers understand their responsibilities as they relate to daily operations.
• Include vendor representatives in refresher training to provide instruction on changes made to hardware and software. Be sure the vendor has a clear understanding of the agency’s mission to ensure message continuity.

• Schedule training for a reasonable length of time. Officers will absorb only a limited amount of instruction. Also, lengthy training sessions may unnecessarily keep officers from their supervision responsibilities.

• Maintain a reasonable instructor-to-staff ratio. There should be an adequate number of instructors, vendor trainers or agency representatives available to assist with questions as they arise.

• Measure training effectiveness by requiring students to demonstrate their mastery of the subject matter. This will help ensure officers perform their tasks properly in the field and also identify training areas that need improvement.

• Ensure that students have all necessary tools for training, including agency-used equipment, desktop or laptop computers and vendor-specific website access. Provide written materials, such as current agency policies and procedures and vendor operation manuals.

• Provide troubleshooting tips on common problems.

• Ask training participants to complete evaluations of training effectiveness.

• Identify additional training needs.

Managing Tracking Evidence

Tracking evidence management is the control of physical and electronic evidence related to a crime or event involving a person who is being monitored electronically. Best practices for managing participant tracking evidence require the establishment of protocols and procedures based on state and federal laws as well as agency departmental guidelines. This section discusses general aspects of evidence management that your agency should consider when establishing a participant tracking evidence management policy.

This section outlines three areas of evidence management:

• Physical evidence.

• Electronic evidence.

• Testimonial evidence.

Physical Evidence. Physical evidence can be introduced in the form of an object. Examples of physical evidence typical to OTS may include:
• **Tracking device:** In some cases, it may be helpful to have the actual tracking device available as evidence. Your agency should establish a policy to determine which devices must be saved as evidence. In some cases, your agency may want to have the device available for independent testing and as physical evidence to display to the jury.

• **Straps:** Save all damaged straps as potentially valuable evidence; tool mark evidence may show how the strap was cut or removed.

• **Tamper evidence:** Tamper marks on a device or attaching components can demonstrate a participant’s intentions.

• **Photographs:** Photographs of tamper attempts and photos identifying the device on the participant may be helpful during proceedings.

• **DNA evidence:** Tracking devices worn by a participant will provide DNA evidence. Agencies should establish protocols to determine when and whether to preserve DNA evidence. In some cases, failure to preserve DNA evidence may prohibit introduction of tracking data as evidence.

• **Documents:** Provide copies of court orders and documents that establish the legal authority for participant tracking. Copies of agreements signed by participants may also be helpful, especially if the document specifies that tracking data can be used in the event the participant is charged with a violation or new crime.

**Electronic Evidence.** The data recorded by and transmitted from an OTS device are considered electronic evidence. Agencies should establish protocols, in consultation with the vendor, for recording and storing copies of original data. The chain of custody of electronic evidence is very important. In most cases, the OTS vendor is the holder of the data. The chain of custody must address the manner in which the evidence is stored to prevent tampering. When establishing electronic evidence protocols, agencies should consider:

• How long will the evidence be available online or by request?

• Should a copy be made of the participant’s tracking points?

• Who will testify from the OTS vendor as the holder of the data?

Agencies should also consider establishing a testing procedure for devices involved in a crime or violation. At trial, defense attorneys often bring up the lack of accuracy testing. Establishing a simple accuracy test for tracking devices involved in crimes or violations will help to validate a participant’s tracking points. For example, displaying the aerial/satellite view of the plotted
Selection and Application Guide to Offender Tracking Systems

points of a stationary tracking device placed in the center of a football field can demonstrate the relative accuracy of the system. (See additional information in Equipment Trials in Chapter 2).

**Testimonial Evidence.** Any evidence given in writing or speech is considered testimonial evidence. Your agency should establish protocols to document testimonial evidence at every stage to support its accuracy.

Tracking events that should be documented include:

- Who last placed the tracking device on the participant?
- Who investigated tamper alerts involving that participant’s device?
- By whom and when was the last inspection done on the device prior to the crime or violation?
- Who removed the tracking device following the crime or violation? Did the device appear to have been tampered with prior to removal? Was the device properly fitted on the participant?
- What, if any, statements did the participant make about the violation or crime?

**Data Retention Considerations**

Agencies should consider data retention and access issues when developing a contract with an OTS vendor. Your agency’s data retention policy should address the legal issues and cost implications surrounding the retention time, archiving rules, formats, and permissible means of storage and access. Federal, state and local government laws or policies may require that certain data be maintained for a specific number of years. In addition to the length of time the information is stored, your agency should also consider the format in which it is stored and the process of obtaining access to the data. As part of their contracts, most agencies will negotiate the length of time that OTS data will be available online and an additional length of time the data will be available on request. For example, agencies will often require that participant tracking data be available online for a minimum of one year and be available on demand for five years.

Agencies should also take special care to develop protocols for information considered evidence due to the length of time cases can be on appeal. Access to current data is not enough.

Your agency should consider obtaining access to the software necessary to view the data in the future. You may consider including a requirement in the contract to provide access to the necessary software for a specific number of years after the expiration of a contract.
Legal Considerations

Agencies should consider legal issues, including relevant legislation, regulation and case law. This section summarizes key points to consider when planning an OTS program. This information provides reference material only and is not intended to provide legal advice. Agencies should consult legal counsel before starting an OTS program.

Key points to consider:

Legislative/Regulatory Considerations
- State regulations and legislation.
- Legal authorization for offender tracking.
- Legal liability.
- Legal authority to recover monitoring costs.
- Legislation regulating tampering with tracking devices.

Data Considerations
- How data is stored.
- Where data is stored and who has custody.
- Length of time data is stored.
- Data security.

Location Tracking Considerations
- What location tracking technology was used.
- Limitations of the location tracking technology.
- Could the tracking points be wrong and, if so, why?

For more information on legal considerations, refer to Appendix B.

Media Relations

Managing media relations involves working with various media organizations to inform the public of your agency’s mission, policies and practices in a positive, consistent and credible manner. The main goal of media relations is to maximize positive coverage and minimize negative coverage, especially during critical incidents. An effective media response plan should
provide the necessary structure for managing and effectively communicating during a critical incident.

Effective media relations strategies should start before a critical incident occurs. Agencies that provide periodic proactive updates to the media are more successful in dealing with the media when a potentially negative incident occurs. Building relationships with the local media is vital to effectively managing critical incidents.

- Do not wait until something potentially negative happens to develop strategies.
- Provide a press release when the OTS project is being initiated.
- Do not oversell the program or equipment capabilities.
- Emphasize that OTS equipment is just one of many tools.
- Create a media packet before any incidents occur.
- Establish a media liaison or public information officer for coordinating all media responses and releases.
- Provide positive stories to the media, such as solving a crime using crime scene correlation, or locating and arresting a sex offender lurking around a school.
- Have statistics available, such as the total number of participants being monitored, the percentage of participants who remove their monitors and the agency’s success rate.

**Planning for Effective Media Relations During Critical Incidents.** Critical incidents are unplanned but inevitable. The negative publicity that an organization receives as a result of a critical incident can have far-reaching effects. Your agency needs a response plan to deal with the media so it can manage and effectively communicate during a critical incident. When a critical incident occurs, many agency managers will be involved in the response. Designating a media liaison or public information officer can help an organization get through the incident without additional damage caused by misinformation and speculation.

The media also can play a critical role in locating participants who abscond from an OTS program. Providing media outlets with wanted posters can quickly generate information that can lead to an arrest.

Cooperating with the media provides an organization with a number of important benefits that far outweigh the advantages of denying them access. In particular, it gives your agency an opportunity to provide its side of the story.
Protecting Data by Controlling Access to Software

Most OTS manufacturers offer web-based software that allows authorized users access to perform necessary tasks. Most systems provide security features to help protect tracking data; however, your agency should develop policies and procedures to guard against outside attack as well as to ensure only authorized internal users can view data. Agencies may be tempted to disable these security features because they may be inconvenient for some users. However, this could result in unauthorized access to your tracking software and compromise the integrity of the program.

Password Strength. Password strength is a measure of the effectiveness of a password in resisting guessing and brute-force attacks. In its usual form, it estimates how many trials an attacker who does not have direct access to the password would need, on average, to gain access. The strength of a password is a function of length and complexity. Using strong passwords lowers the overall risk of a security breach; however, strong passwords do not replace the need for other effective security controls.

A strong password is only as good as the strength of the authentication system software. Frequent incorrect password submissions should result in a user’s being locked out and a supervisor’s being required to reset the password. You should not store passwords in locations easily accessible to unauthorized users.

Password Considerations

- Avoid any password based on usernames, relatives or pet names, or biographical information.
- Include numbers and symbols if allowed by the system.
- If the system recognizes case as significant, use both capital and lower-case letters.
- Avoid using the same password for multiple sites or purposes.
- If you write your passwords down, keep the list in a safe place.

Password Policy. Establishing a policy that requires a password to be changed frequently may result in officers choosing weaker and more vulnerable passwords. For example, a user may choose “Password1,” “Password2” and “Password3” as successive passwords. Although such a password selection method is easy for the user to remember, it leaves your agency extremely vulnerable to an attack. If an agency must choose between reset frequency and password strength, give strength priority.
Inactivity Lock. *Auto-lock features* force a software program to lock after a period of inactivity. Agencies often overlook this important feature. The ability to determine the period of time before a software program locks allows agencies to consider security versus the inconvenience of users being forced to log back in.

Employee Separation. Agencies should develop a procedure to identify their internal and external users who have been terminated or transferred. Remove users who no longer need access to OTS data as soon as possible and include removal of access to OTS software as a checklist item for separated or transferred employees. Some agencies also run a usage report and suspend access for users who have not accessed their account for a predetermined period.

Measuring Offender Tracking Program Outcomes

When an agency uses public funds, there is an obligation to demonstrate that tax dollars have been invested wisely. If your agency does not keep performance measures, the lack of accountability to the public may result in a loss of good faith and, eventually, the elimination of funding.

To measure a tracking program’s success, your agency needs a clear understanding of the desired outcome. Although one agency may choose to use OTS technology to reduce institutional overcrowding, others may use it to enhance supervision of their highest risk community participants. Obviously, how these programs measure success will differ.

If your agency’s objective is to enhance public safety through tracking high-risk participants in the community, success measurements could include the number of leads from crime scene correlation or a comparison of new crimes in the monitored population to a sample population that is not monitored. If the program is helping participants avoid criminality, the measures should reflect this important public safety benefit.

Some programs use tracking technology in domestic violence cases. These agencies could report the number of early warning alerts sent to victims resulting in the avoidance of participant-victim encounters. Another measure may be fewer re-victimization incidents during the evaluation period when compared to a time period when the technology was not used.
Chapter 4. Operational Considerations

Your agency should be aware of numerous operational issues that can impact the success of an OTS program. This section will help agencies identify these topics and provide a general understanding of how they can affect a program.

Matching Technology to Offender Type

Selecting the most appropriate OTS technology is critical. Considerations for matching the participant with the technology include, but are not limited to, the following:

- Program objectives.
- Conviction types, if applicable.
- Level of response.
- Staffing resources.

Program Objectives. Reviewing program goals and objectives can help identify the appropriate technology. For example, a program to reward the good behavior of lower risk participants being released from confinement may choose a passive technology while an agency may choose active technology for higher risk participants.

Conviction Type and Offender Risk. Different crime conviction classes (e.g., sex, drugs or gang participations) and offender risk levels can require unique supervision strategies and case management requirements. Remember that the time needed to complete tasks associated with location tracking is in addition to that needed for all other supervision requirements of the case plan. Carefully review staffing levels to ensure all objectives relating to the supervision of a specific class of participant can be realistically met.

A few specific considerations for choosing the appropriate technology based on conviction type include:

- Many juvenile programs have selected one-piece devices due to the perceived increased likelihood of juveniles misplacing or forgetting to carry components of a multi-piece system.
- Some vendors now offer mobile exclusion zones, a tool that may be very useful in the supervision of gang members as well as in cases where the participant has demonstrated violence toward a particular individual (e.g., domestic violence).
Always choose active technology when your agency wishes to be able to alert a victim of the proximity of a tracked participant.

**Staffing Resources and Agency Level of Response.** As discussed in Chapter 3, your agency must determine a level of response to notifications/violations. Active tracking technologies usually provide prompt notification of events. Your agency can choose differing levels of vendor involvement in the response process. Obviously, additional services provided by a vendor will result in increased costs. If an agency intends to use its own personnel for immediate responses to selected tracking violations, staffing resources must be continuously available. If the agency does not have the ability to provide this level of response, passive tracking technology may be more appropriate. Violations committed by passively tracked participants are typically provided to an agency at the beginning of each business day.

**Other Considerations.** The complexity of the chosen technology can impact workload. Ease of installation and required enrollment activities may vary significantly from vendor to vendor. The time difference may be negligible, but agency staff may have a strong preference for a certain approach. Consider allowing staff to become familiar with the technologies under consideration prior to signing a contract. Considering staff input may help create a program that is better received and, as a result, more effective.

**Ergonomic Considerations**

Your agency should consider several physical characteristics when selecting an OTS technology.

- **Size and weight.** Give particular attention to the body-attached equipment. Most devices on the market weigh less than 300 grams and have a displacement of 200 ml or less. Devices larger than this may cause unnecessary discomfort to the wearer, especially if the participant is a juvenile. As new technology develops, agencies may want to balance size with the potential for increased functionality that comes with a larger device.

- **Protrusion.** A body-attached device that extends outward significantly from the skin could cause the device to repeatedly bang against objects as the participant moves. This could cause injury and increase the incidence of equipment breakage. When fitted properly, most OTS body-attached devices will protrude less than 40 mm from the skin’s surface.

- **Emergency Removal.** Under normal conditions, only authorized personnel should remove the body-attached device, using specialized equipment provided by the OTS vendor. Your agency should very carefully consider how a first responder would remove a body-attached device from a participant in the event of a medical emergency. If an
injury occurs to the extremity on which the device is attached, paramedics and/or emergency room personnel need to be able to remove the device quickly using standard, readily available tools. If medical personnel cannot easily remove the device and alleviate any swelling and circulation loss in the injured extremity, serious medical complications can result. Careful selection of body-worn device and attaching components can help prevent such incidents and also limit your agency’s exposure to liability.

- **Allergens.** Although most manufacturers of OTS equipment select materials that do not contain known allergens, your agency may find a few cases where the external surfaces of a body-attached device cause an adverse skin reaction. Ask potential equipment providers which materials they have selected and how much testing they have done to ensure the devices will not likely cause allergic reactions. At this writing, a helpful contact allergen database can be found at: [http://contactallergy.com/](http://contactallergy.com/)

**Installation**

Your agency should develop a standard operating procedure for proper installation of OTS devices. When considering the location for device installations, make the safety and security of personnel and equipment a priority. Stored spare parts should be kept in a location to which participants do not have access.

Install the device in a manner that will not allow the participant to see the process. You may elect to have the participant face a wall with both hands on the wall at shoulder height while placing one knee on a chair or bench. This procedure allows for installation of the device out of participant view while enhancing staff safety. Your agency staff should follow a similar process for removal.

Follow the manufacturer’s recommendations. Proper fit is important to prevent unauthorized removal. A too-tight device can cause skin irritation, resulting in discomfort to the wearer. A device that is too loose could allow for its removal without detection. Agencies should also consider proper documentation of the installation to include who installed the device, on which body part the device was installed and the strap size or measure.

**Participant Initial Orientation**

Providing appropriate training to participants of an OTS program is critical for obtaining positive outcomes. Agencies must balance how much information to give the participant with providing an adequate level of understanding of the technology and equipment. Participant training considerations can include an overview of the tracking technology, equipment installation, equipment charging instructions, equipment cleaning and maintenance, curfews and geographic
restrictions, crime scene correlation, and “dos” and “don’ts” while being monitored. Each agency must develop participant training protocols that will effectively educate the participant to ensure program and agency objectives are met.

Experience has shown that participant orientation to OTS technology and agency expectations reduces initial problems. If participants understand how the hardware attains satellite triangulation, it can cut down on the initial notifications staff receive and also provide participant accountability for noncompliance. Most systems provide some type of signal to warn participants of noncompliance situations such as low battery, entering an exclusion zone and lack of GPS signal. Make participants aware of these signals and what they mean. If your agency expects participants to acknowledge notifications and text messages, they need to know how to complete the acknowledgements.

Consider delivering this training using two or more learning styles, which may include audio-visual instructions, verbal instructions, written instructions and/or demonstrative/practice by doing. Take steps to ensure participants with handicaps and language barriers receive proper training. Consider allowing a participant’s family members to attend the training, especially in the case of a young or special needs participant. (Participant tracking can have a significant impact on family members.)

**Equipment Charging.** Charging compliance is one of the most common issues agencies face while managing an OTS program. Your agency can curtail noncompliance with charging requirements by implementing good charging protocols. The participant should receive instructions on the proper procedures for charging the device, including the time of day to charge, the length of time to charge and activities forbidden while charging, such as sleeping or bathing.

**Curfews and Geographic Restrictions.** Many OTS participants have judicially imposed curfews and geographic restrictions (inclusion and exclusion zones). The participant should acknowledge receiving and understanding the location and times for such restrictions. Give participants a map indicating the boundaries for geographic restrictions.

**Crime Scene Correlations.** Agencies that use tracking data for the purpose of crime scene correlation may consider notifying the participant of this feature in writing. Preventing or deterring crime is the ultimate goal of crime scene correlation; therefore, agencies should instruct participants on how the crime scene correlation process works in order to underscore the likelihood of being caught if they engage in illegal activity.
**Equipment Cleaning.** Using manufacturer’s recommendations, your agency should provide the participant with cleaning instructions to ensure the device stays clean and the affected skin area does not become irritated.

**Disabilities and Language Barriers.** Your agency should develop participant training with disabilities and language barriers in mind. Consider having instructions available in multiple languages in addition to considering mental health and educational levels.

**Additional Offender Training Considerations.** Your agency should use caution when developing participant training to ensure that the information provides clear guidelines without inadvertently helping participants devise circumvention techniques.

- Withhold sensitive information from the participant such as how often a location point is plotted or the frequency with which data points are uploaded to the monitoring center.
- Notify participants verbally and in writing of the possible ramifications of violations.
- Give participants instructions on how to notify the agency immediately if they experience any issues with the equipment.
- Give participants directions on what to do in an emergency situation such as a loss of power, pending weather conditions or emergency relocations.
- Provide participants with information on the consequences of removing or destroying tracking equipment.

**Inspection, Care and Maintenance**

Your agency should inspect all equipment assigned to a participant on at least a monthly basis. Document the inspection in writing and include:

- Proper fit of equipment.
- Signs of damage, tamper, cracking or wear.
- Any signs of allergic reaction, such as swelling, inflammation or redness.
- Inspection of electrical cords and plugs for signs of wear.

The manufacturer should provide the agency with proper cleaning instructions for all participant equipment between uses. Properly disinfect equipment used by each participant before reissue. Some agencies soak reusable straps and tethering components in a container of disinfectant solution to prevent the spread of disease. Other agencies use dishwashers with high temperature settings to disinfect equipment.
Selection and Application Guide to Offender Tracking Systems

Do not forget to properly clean auxiliary equipment such as chargers and beacons prior to reassigning them to new participants. If the manufacturer does not provide specific cleaning instructions, discuss with the manufacturer the method your agency plans to use prior to implementing that equipment cleaning/disinfecting protocol.

Factors That Impact Location Tracking

Understandably, agencies want to procure equipment that tracks the locations of participants with great precision. In fact, there are often expectations that OTS equipment should always be accurate and reliable. Unfortunately, tracking technologies have limitations that impact accuracy under certain conditions. Some of these limitations are out of the manufacturer’s control, whereas component selection and manufacturing techniques impact others.

GPS drift is a common way of describing the phenomenon of tracking points that are plotted inaccurately, often erring toward a single direction. A variety of factors can cause this, including changes in satellite positioning, receivers operating in obstructed environments and satellite and/or algorithmic errors. Any one (or a combination of) these factors can make it appear that a stationary tracking device is moving. Also, these factors may erroneously show a single location point plotted a significant distance from others (an outlier). Well-trained employees can usually recognize these errant location points, but they sometimes can be confusing and problematic. When the accuracy of location points is in question, your agency should consult the technical staff of the vendor or service provider for clarification.

When your agency is evaluating the accuracy of an OTS device, it is important to understand all of the many variables that can impact accuracy. To better control the variables that can impact accuracy, evaluate side-by-side the devices under consideration for use.

A discussion of the variables that can affect accuracy follows.

Limited GPS Signal Reception. Reception of signals from a minimum of three GPS satellites is required to calculate location. The greater the number of satellite signals received, the more accurate are the location coordinates derived. In ideal conditions when eight or nine satellite signals can be received, location can often be calculated within several feet. However, much of the time structures, foliage, cloud cover, precipitation and natural land formations (e.g., canyons) block signals. Tracking devices in the heart of metropolitan areas can have a limited view of the sky due to surrounding skyscrapers. These “urban canyon” environments have proven to be very challenging for tracking devices relying on GPS. Reducing the number of satellites received under any of these adverse conditions can cause accuracy to decrease significantly. The same
principle holds true with other location-based services. As more location signals are received by the tracking device, the reliability of the calculated location increases.

Location of Satellites. When the origins of the location signals (i.e., coming from GPS satellites) are in near alignment, accuracy can be adversely impacted. The most accurate location calculations occur when the location signals come from disparate locations.

Multi-path. Location is usually calculated by analyzing the time difference of arrival of synchronized signals originating from a number of transmitters whose precise positions are known. This assumes that the path of the signals follows a straight line from the transmission source to the receiver on the tracking device; however, this does not always occur. A transmission may arrive at the receiver after reflecting off certain surfaces, causing a delay in the signal’s arrival. Also, that same signal may or may not have found a direct path to the receiver. This phenomenon is known as the multi-path effect and can cause significant error in location calculations. Buildings with reflective surfaces and bodies of water commonly cause this effect.

Solar Conditions. GPS-based location systems are susceptible to occasional periodic location error when solar conditions change. The signals transmitted from the orbiting GPS satellites must pass through the earth’s ionosphere. After a significant solar event, such as a flare, the ionosphere can become electrically charged. This can cause the path of the location signals passing through the ionosphere to bend, resulting in a delay in the arrival of the signals to a tracking device. Because location is calculated by the signal’s time of arrival, accuracy can be significantly impacted.

Antenna Selection, Orientation and Position. Each OTS manufacturer carefully considers which antenna is used within a tracking device and positions that antenna in a manner believed to maximize reception. Some vendors may make better antenna selections and may better position those antennas within the device, resulting in an increased sensitivity to the incoming location signals. Increasing the number of location signals received enhances accuracy.

Kalman Filters and Precision Algorithms. Not all location information plotted on a map is derived from raw data. Often, filters and precision algorithms adjust the location information. A Kalman filter, for example, uses statistical probabilities to produce location values that tend to be closer to true values than their associated calculated values. These filters are often built into chipsets rather than created by the OTS manufacturer.
OTS manufacturers may choose to use additional mathematical models in an attempt to improve the accuracy of plotted location points. *Precision algorithms* are computations that typically consider the pattern of previous location points to predict and then plot the next logical point. For example, if a participant is sleeping in bed, location points should consistently be plotted in a tight cluster. If there is suddenly a significant variation from that pattern, a precision algorithm may adjust the raw data and plot the location closer to the well-established cluster. If the raw data continues to show a new location, the precision engine will eventually adjust the incoming plotted points to reflect the new position. By eliminating stray location points caused by any one of a number of degrading factors, precision algorithms can significantly reduce false zone infractions. However, systems that use this methodology may be slow to detect an actual sudden change of location and could potentially delay an agency from receiving critical information.

**Assisted GPS.** Some GPS systems use strategically positioned ground stations. Because the exact location of each station is known, the error in the GPS-derived location can be easily identified. A correction can then be broadcast to any GPS devices near these sites.

**Advanced Forward Link Trilateration (AFLT).** AFLT calculates location by measuring the time difference of arrival of signals from nearby cell towers. Because AFLT uses cellular signals (which are more penetrating than GPS), this method of participant tracking is more effective at providing location information indoors and in other RF-compromised environments. AFLT requires the availability of a minimum of three cell towers, with the number of towers and the distance and alignment of towers affecting the accuracy. Typically, the accuracy of AFLT is not as precise as GPS tracking, but can usually provide location within 50 meters in environments served by numerous cellular towers.

In the United States, only code division multiple access (CDMA) cellular networks can use AFLT for positioning. Therefore, your agency should ask potential vendors about the cellular network their equipment uses and whether they offer AFLT positioning. Because of its less reliable accuracy, AFLT is usually used as a secondary location methodology when GPS is unavailable. AFLT should not be confused with the far less accurate cell tower ID location methodology, which only identifies the cell tower used to communicate information to the data center.

**Data, Monitoring and Alert Centers**

Sometimes OTS terminology is misunderstood and misused. This can cause confusion in the procurement of OTS services and even result in operational problems affecting the success of a program. This is especially true with the confusion over the terms “data center,” “monitoring
center” and “alert center.” The following section defines and explains these terms, and helps agencies understand what is expected at these important centers of activity within an OTS.

**Data Center.** A *data center* is a facility equipped with, or connected to, one or more computers used for receiving, processing or maintaining participant tracking data. A vendor typically operates a data center on behalf of the agencies with which it has contractual relationships. Usually staffed by a small number of highly technical employees who have little interaction with agencies, a data center is where participant tracking information is received, processed and stored. When evaluating a vendor’s data center, consider the following:

- The center should be capable of uninterrupted 24/7/365 operation.
- The center should have a backup power supply capable of sustaining operations indefinitely.
- The vendor should have a written disaster recovery plan.
- The vendor should have a secondary data center capable of seamlessly continuing data collection and processing in the event of an emergency. This secondary center should be located where the probability of being impacted by the same incident is extremely low.
- The vendor should have written security policies and procedures for network security, data transmission integrity, data storage and physical security.
- The data center should have a fire suppression system.
- The data center should have an extremely robust firewall in place to protect against unauthorized access to data.
- The vendor should check employees for a criminal history prior to hiring them, with periodic rechecks thereafter.

**Monitoring Center.** A *monitoring center* is a designated location where participant tracking information is received, and alerts responded to, in accordance with a protocol established by an agency. Typically, an OTS vendor operates a monitoring center on behalf of the agencies with which it has contractual relationships. It should be located in a secure environment and staffed by carefully selected individuals who are well trained to respond to tracking situations according to the protocols and levels of service requested by the agency. When evaluating a vendor’s monitoring center, consider the following:

- The center should be capable of continuous 24/7/365 operation.
The vendor should have a written disaster recovery plan.

The monitoring center should have a backup power supply capable of sustaining operations for a minimum of two days.

The monitoring center should have a fire suppression system.

The monitoring center should have sufficient physical security.

The vendor should check employees for a criminal history prior to hiring them, with periodic rechecks thereafter.

**Alert Center.** An alert center is a designated location where agency employees respond to certain events reported to an agency, especially during hours that assigned supervising officers are not on duty. Alert centers often are part of an agency’s strategy to maintain 24/7 response capabilities while having a majority of the employees assigned to the OTS program work traditional hours. Alert center employees triage violations reported by the vendor in an attempt to resolve as many incidents as possible without having to immediately bring them to the attention of an assigned officer. If your agency is contemplating the use of an alert center, it should consider the following:

- Is there sufficient funding to staff an alert center during all nontraditional working hours? (Some alert centers operate on a 24/7 basis.)
- Policy protocols should clearly delineate what alerts need to be brought directly to the attention of a supervising officer.
- Consider developing scripts for alert center employees to follow when responding to the most common alerts. For example, scripts could include instructions for a participant to follow when a battery is low on power or directions to a participant who is late for a curfew.
- Select alert center employees carefully and screen them for criminal history.
- To address safety and accountability concerns, staffing levels should usually provide for two or more employees during hours of operation.

**Information and Data Exchange**

Agencies often overlook the format in which OTS data are maintained. Vendors store data in a variety of different formats, sometimes making the exchange of information difficult. Your agency should consider how data are maintained for the following two reasons:
• **Changing Vendors.** Many agencies change vendors during the life of their OTS program. Unless your agency makes provisions in its contract, much of the historical tracking data may be lost when you switch to a new vendor. Agencies should anticipate this and make arrangements to protect data usability. Keep abreast of emerging data standards and ask vendors to provide historical data in the most universally accepted format on conclusion of a contract. When considering a new provider, ask vendors if they will be able to display the agency’s historical data on the new software.

• **Crime Scene Correlation.** It is not uncommon for a number of criminal justice agencies within the same metropolitan area to use the services of a variety of different vendors. Because there are no uniform data exchange protocols in place, it can be very difficult for these agencies to perform automated crime scene correlation. Data from the various OTS vendors must be run independently, causing a significant increase in effort and delays in obtaining correlation results. Criminal justice agencies within the same metropolitan area should communicate with each other to plan for the most efficient means of collecting and providing location data to other area agencies. (For additional information, refer to Crime Scene Correlation later in this chapter).

**Circumvention Considerations**

OTS participants are often antagonistic toward their monitoring requirements and may use creative means to circumvent tracking. Fortunately, most manufacturers have incorporated highly effective tamper-detection technologies into their tracking systems.

The names given to the various circumvention alerts vary from manufacturer to manufacturer. However, they typically include most, if not all, of the following:

- Cut strap.
- Proximity alert.
- Open case.
- Bracelet gone.
- No GPS.
- Tracking gap.
- Low battery.
- Communication failure.
Temporary interruption of location and/or communication signals generates some of these alerts (e.g., bracelet gone, no GPS, tracking gap) whereas others occur after a participant physically alters the device (e.g., cut strap, proximity alert). A low battery (which may result in a communication failure) can be intentional to allow a participant to hide his/her location from the tracking system after the device has lost power. Keep in mind that many devices cannot record and/or report other tamper events after power has been lost, even after the device has been recharged. Because of this, your agency should have an inspection protocol in place to ensure that devices are properly attached to the participant and have no obvious signs of damage or evidence of tampering.

**Routine Inspections.** Inspect all equipment assigned to a participant on at least a monthly basis. Your agency should do this randomly without giving the participant advance notice. Because equipment varies from vendor to vendor, a uniform inspection protocol is not practical. The manufacturer should provide specific instructions on how to conduct periodic inspections. However, all inspections should include several common elements.

- Check the fit of the body-attached device. If it differs from the installation fit, consider unauthorized removal as a possible cause. Keep in mind that ankle sizes may vary due to swelling and some strap stretching may occur. However, excessive strap stretching may be a sign of intentional tampering. Participants sometimes apply heat to straps to make them more pliable. Officers should look for melted or charred areas.

- Document the specific body part on which the officer installed the device. Without this documentation, obvious evidence of removal and reattachment could go undetected.

- Check for any signs of damage caused by impact or normal wear. Cracks on the casing could eventually result in equipment failure if water ingress occurs. Inspect the strap for signs of cracking or fatigue caused by long-term use. The presence of glue anywhere on the device may indicate that intentional tampering took place. Remove the device from the participant in a manner that will not compromise further inspection. This may require cutting the strap midway between its connection points.

- Examine the participant’s skin where the device is attached. Look for any signs of allergic reaction, such as swelling, inflammation or redness. Although most manufacturers use materials that are unlikely to cause allergic reaction, documented cases have occurred and could create a serious health concern. If this occurs, seek advice from a medical professional. Look for injury to the attachment area caused by other factors. Excessive chafing, bruising and tenderness could evolve into more serious medical
concerns if allowed to continue. In most cases, attaching the device to another part of the body will remedy the situation.

**Inspection for Cause.** Prior to assigning equipment to a participant, document any significant damage or tool marks. Any time your agency receives an alert for a tamper, inspect the equipment within 24 hours. Never assume such alerts are “false alerts.” Obvious signs of device tampering include a cut strap or missing, broken or damaged attachment parts. To avoid detection, participants may attempt to glue broken pieces back together. Hairline cracks or the presence of glue anywhere on the device may indicate a tamper attempt.

Depending on the equipment used, an officer may detect less obvious signs of tampering. Look for any tool marks at the fastening points. Participants sometimes use screwdrivers, pliers or other small tools to force equipment away from the strap. Such circumvention attempts almost always leave tool marks on the device. If your agency finds no evidence of tampering, especially after a second false tamper alert, return the device to the vendor and request a thorough inspection. You should also inspect equipment immediately any time an officer receives information that a participant has been at a location not consistent with the tracking location data.

The vendor should provide the agency with a device removal procedure that will not compromise any evidence of participant removal and reattachment. In many cases, this may involve removing the device from the participant by cutting the strap midway between its connection points. If your agency determines that a tamper has occurred, fully document the incident and take steps to preserve the physical evidence for prosecution.

**Crime Scene Correlation**

*Crime scene correlation* links crime or incident data with location points from OTS devices. This growing technique can enhance public safety efforts.

Most law enforcement agencies keep an electronic record of reported crimes, including dates, times and location. Crime locations are converted to longitudes and latitudes in a process known as geocoding. If a participant was at, or near, the scene of a crime when it occurred, the participant might be looked at as either a suspect or a potential witness. Conversely, participants may be eliminated as suspects if tracking points indicate that they were elsewhere when the crime occurred.

The value of crime scene correlation lies in its ability to automatically cross-reference large databases and quickly develop a list of potential suspects. Criminal justice agencies can set the
parameters for a match (e.g., distance between participant’s location point and the reported crime scene, difference in time between the participant’s presence at that point and the reported crime).

Most vendors offer basic software that performs simple crime scene correlation. Instead of comparing large databases of crime scene information with the known tracking points of multiple participants, the basic software offers reports that indicate whether any participants were at a designated location during a designated time period. Some manufacturers offer automated crime scene correlation that allows agencies to upload crime data and receive automated reports for potential crime scene hits.

The use of a crime scene correlation program allows law enforcement agencies to quickly identify participants who choose to continue committing crimes while wearing a monitor. Participants who understand the effectiveness and efficiency of this technology will be less likely to commit criminal acts because of the high likelihood of getting caught. Participants have three choices: commit crimes knowing they will be looked at as suspects, discard the tracking device and become fugitives or choose to refrain from criminal activity while being monitored.

Another aspect of crime scene correlation is the comparison of interest point mapping with OTS data. Interest point mapping correlates any physical location that may be of interest to law enforcement or corrections with OTS data. This process is especially helpful in identifying who frequents high drug-use and gang areas. Interest point mapping can also identify who frequents pawn shops and known fencing locations.

**Report Considerations**

Each OTS program relies on system-generated reports to monitor participant status and review overall program effectiveness. Because each agency has differing objectives, the reports needed may vary significantly. Your agency should understand what reports it needs and communicate that need to the vendor. Contracts with vendors should include language that allows for the creation of customized reports that meet the agency’s needs.

Consider the following when planning for the development of reports for your OTS program:

- Reports critical to the day-to-day operations of the program should be automatically generated and delivered daily to the appropriate personnel.
- Periodic management reports should clearly show progress made in reaching the agency’s objectives.
Your agency should be able to generate and review monitoring/tracking reports on-screen and print hard copies when necessary.

Your agency should decide whether the reports should be generated in Portable Document Format (PDF), Microsoft® Excel or some other desired format.

Your agency should have procedures in place to request and create new reports according to your specifications.

Battery Considerations

Agencies evaluating an OTS should pay particular attention to the battery life of a tracking device. If a tracking device has an unreliable power supply, the monitoring of the participant may be regularly interrupted. This compromises the integrity of the program and can pose an unnecessary risk to the community. Also, the amount of manpower devoted to addressing battery issues can have a significant impact on agency operations.

Your agency should consider many factors when evaluating batteries. Every OTS manufacturer uses various power management strategies to conserve power, which can make direct comparison of devices challenging. Consider the following when testing an OTS:

- Does the device use a beacon to conserve battery life?
- Does the device use an accelerometer to put the device to rest?
- What is the manufacturer’s recommended charge time?
- What is the manufacturer’s recommended time between charges?
- Does the device use onboard or post-processing to detect violations?
- What is the polling frequency and upload rate?
- Does the device have additional features that consume battery power, such as speakers, two-way communication and lights, or vibration for alerts?
- Is the battery field-replaceable by the agency or does your agency need to return the device to the manufacturer for replacement?
- Does the device change polling and upload intervals when in a tamper mode, zone violation or any other non-compliant events?
- After how many charging cycles does the manufacturer recommend battery replacement?
Participants can intentionally fail to properly charge a device in an attempt to circumvent tracking efforts. (See Inspection for Cause earlier in this chapter.)

**Robustness Considerations**

Virtually all electronic devices are susceptible to failure due to dropping, banging and exposure to moisture. Consumers are typically very careful to protect their electronics from harsh environments to prolong the device’s life and to protect their investment. OTS equipment contains components just as susceptible to failure as any other electronic product. However, tracking participants are much less likely to care for their assigned tracking devices, and often intentionally subject the equipment to environments where most other electronics will quickly fail.

The OTS standard addresses this reality by developing very stringent robustness requirements. Devices should work reliably in a number of extremely harsh environments during the entire period of supervision. Equipment found in compliance with the standard has passed rigorous testing, including shock, vibration and environmental conditions. (For more information, see Sections 6.24 through 6.34 of the standard.)

Although OTS devices will always suffer some failures due to exposure to harsh environments, the standard identifies the most common causes of equipment failure and implements reasonable survivability testing that increases the likelihood of approved devices’ operating reliably for extended periods, even after exposure to a variety of adverse conditions.

**Communication With the Participant**

Your agency should determine the amount of information provided to participants. The level of information provided is based largely on agency preferences. Some agencies feel that as participants receive more information, the likelihood of participant exploitation of the equipment/system increases. Conversely, some agencies believe that as more information is provided to the participant, the more likely the participant will modify his/her behavior and comply with the rules of electronic monitoring increases. Your agency should determine what best fits its needs.

Some types of communication with participants include the following:

- Audible (other than voice) alerts.
- One-way or two-way voice communications.
- Vibrations.
• Text messaging.
• Visual alert notifications.

Some agencies require participants to acknowledge receipt of the communication provided. This allows agencies to ensure that participants receive and comply with alert notifications and instructions. The level of feedback is based largely on agency preference.
Appendix A: Common Terms for Offender Tracking Systems

Acronyms

AFLT: Advanced Forward Link Trilateration.
CDMA: Code Division Multiple Access.
GPS: Global Positioning System.
GSM: Global System for Mobile Communications or Groupe Spécial Mobile.
OTS: Offender Tracking System.

Commonly Used Terms

The definitions provided in this appendix apply to these terms as used in this guide, where applicable. Not all terms appear in the text; they are provided here to help practitioners achieve a common understanding of term definitions. Terms not defined in this appendix or within chapter text are defined using their ordinarily accepted meanings within the context in which they are used.

Accelerometer: Electromechanical device that measures acceleration forces.

Accuracy: Measure or characterization of difference between a participant’s location, as determined and reported by the OTS, and the participant’s actual location.

Active tracking: An offender tracking approach that uses a location system and a communications infrastructure to accomplish near real-time collection and transmission of device location and status data. An active offender tracking system receiving NIJ certification must be capable of providing on-demand location and status information to an agency within three minutes and provide zone and status alerts to an agency within four minutes (assuming the location system and communication infrastructure relied on are working properly).

Ad hoc query/reporting: Approach that permits users to create and execute customized requests for vendor data, and to generate reports that contain the output of such requests.

Administrative privileges: OTS software security permissions that permit agency-level administration of agency employee access to automated OTS data and reporting.

Advanced Forward Link Trilateration: A position location methodology that calculates location by measuring the time difference of arrival of signals received from three or more cellular communication towers, typically within a CDMA network.
Aerial view: A graphical display against a mid-air image of the area over which the tracking points are distributed. Some mapping software may refer to this as “satellite view.”

Alert: (1) Notification that an offender wearing a tracking device has engaged in activity of interest to the supervising entity (e.g., zone breach, tamper), or that a device parameter of interest has changed (e.g., low battery power). (2) Event generated or recorded by an offender tracking system that requires notification to the subscribing agency for possible enforcement action.

Alert center: Designated location where agency employees or vendors respond to certain reported events, especially during hours that the assigned supervising officers are not on duty.

Assisted Global Positioning System: Position location technology that uses data from an available wireless or cellular network to help a tracking device more quickly locate and acquire GPS (see Global Positioning System) signals under poor signal conditions.

Atmospheric conditions: Prevailing meteorological situation, usually expressed in measures of temperature, humidity, wind, clouds and precipitation.

Base station: Receiver that is set up on a known location specifically to collect data for differentially correcting rover files. It calculates the error for each satellite and, through differential correction, improves the accuracy of GPS positions collected at unknown locations by a roving GPS receiver. Also called a reference station.

Battery cycle life: Number of charge/discharge periods, to a specified depth of discharge, that can be sustained before failure to meet specified capacity or performance criteria.

Battery life: Period of operational capability at or above specified capacity after charging.

Beacon: Optional component of an offender tracking system that emits and/or receives radio signals. Used to enhance the accuracy and battery life of an OTS.

Body-attached: Quality of being physically secured to a participant.

Body-worn: Quality of being carried, or of being fastened to an article of clothing worn, by a participant.

Bracelet: Body-attached portion of an OTS device, usually affixed to a participant’s wrist or ankle.

Bracelet gone: See Tether gone.

Care: Cleaning, sanitization and storage of an OTS hardware unit and/or accessories.

Circumvention: Action intended to frustrate or defeat proper OTS device function.
**Code Division Multiple Access (CDMA):** Method for transmitting multiple digital signals simultaneously over the same carrier frequency (channel). Although used in various radio communications systems, its most widely known application is for cellular telephones.

**Cold start:** Operational condition of a GPS receiver when the receiver has no, or inaccurate, estimates of the current time, the receiver’s position or velocity, or the location or visibility of the GPS satellites.

**Communications failure:** Inability to establish a connection with the monitoring center or data center to upload data.

**Condensing humidity:** Water in the air that is transformed from a gaseous to a liquid state due to a combination of temperature and pressure changes. During testing, condensing humidity tests usually consist of temperature cycling in high relative humidity air that pulls ambient air into the device and induces condensation on all surfaces.

**Crime scene correlation:** Automated process of comparing stored offender tracking data with the known location(s) and time(s) of crimes in order to determine whether one or more tracked offenders were at or near the location of the crime(s) when it/they occurred.

**Data center:** Facility equipped with, or connected to, one or more computers used for receiving, processing or maintaining OTS data.

**Deduced (dead) reckoning:** Process of estimating current position based on a previously determined position and advancing that position based on known or estimated speeds over a period of time.

**Drift:** Common way of describing the phenomenon of GPS tracking points that are plotted inaccurately, often erring toward a single direction. This can be caused by a variety of factors, including changes in satellite positioning, receivers operating in an obstructed environment, and satellite and/or algorithmic errors (see outlier).

**Encryption:** Protecting data in transit from unauthorized use by applying a mathematical algorithm to render the data unreadable without the use of a decryption key.

**Ephemeris:** Predictions of current satellite position transmitted to the user in a data message.

**Event:** Any incident recorded by an offender tracking system that is time-stamped, logged and reportable.

**Exclusion zone:** User-defined area outside of which a tracked offender must remain during specified periods.
**Fiber optic:** Cable containing one or more glass (or plastic) threads. These elements are typically individually coated with plastic layers and contained in a protective tube suitable for the environment where the cable will be deployed.

**Field-replaceable system-level components:** OTS hardware elements that can be replaced by the agency without destructively opening the hardware component casing (e.g., batteries, straps).

**Firmware:** (1) Fixed, usually rather small programs and/or data structures that internally control various electronic devices. (2) Software stored in read-only memory (ROM) or programmable ROM (PROM) that often is responsible for the behavior of a system when it is first switched on.

**Fix:** Finding of the location of a tracking device.

**Free-form zone:** User-defined irregular polygon that permits introduction of an unlimited number of nodes to produce a highly customizable, asymmetrical shape.

**Geocoding:** Process of determining associated geographic coordinates from other data, such as street addresses or postal codes, and using those coordinates for mapping purposes.

**Geographic Information System (GIS):** Computer-based technology for retrieving, storing and organizing data based on its location on a map.

**Global Positioning System (also Global Positioning Satellite System):** (1) Satellite-based location service created by the U.S. Air Force. (2) Satellite-based positioning technology that, with differential correction, can yield high accuracy.

**Global zone:** User-defined area that can be broadly applied to multiple participants.

**Hot start:** Operational condition of a GPS receiver when the receiver has valid time, position, almanac and ephemeris data, thus enabling rapid acquisition of GPS satellite signals.

**Humidity:** Amount of water vapor in the air. The most common description of humidity is of *relative humidity*, or the amount of water in the air compared with the amount of water the air can hold, given the temperature at the time of measurement.

**Hybrid tracking:** Approach in which the device operates in passive tracking mode while the wearer is compliant with restrictions, but switches into active tracking mode when the wearer is noncompliant.

**Hypoallergenic:** Design or material quality that reduces or minimizes the occurrence of an allergic response, often through the use in production of relatively few or no potentially irritating substances.

**Institute of Electrical and Electronics Engineers (IEEE) 802:** Family of standards related to networks that carry variable-size packets, such as local area networks or metropolitan area
networks. The most commonly known 802 standard is 802.11, which relates to wireless local area network computer communication in the 2.4 and 5 GHz frequency bands.

**Inclusion zone:** User-defined area within which a tracked offender must remain during specified periods. Inclusion zones are usually defined using product-specific software, and offender noncompliance generally results in delivery of an alert to the supervising agency.

**Jamming:** Use of an electronic device to disrupt communications by overriding incoming transmissions at the receiver.

**Latitude:** First component of a spherical coordinate system used to record positions on the Earth’s surface. It indicates the angular distance north or south of the Earth’s equator, measured through 90 degrees.

**Layers:** Means of organizing and managing map data by type. Features, such as bodies of water and railroads, can be contained on separate layers for easy map creation and maintenance.

**Location point:** Geographic spots derived by a positioning service.

**Longitude:** Second component of a spherical coordinate system used to record east-west positions on the Earth’s surface, measured in degrees as the arc or position of the Earth’s equator intersected between the meridian of a given place and the prime meridian.

**Low battery:** Reportable OTS device power status that indicates a pending loss of power.

**Map view:** Graphical display of tracking points against a street map of the area over which the points are distributed.

**Model:** OTS manufacturer’s variant design of a particular product, with unique specifications and characteristics that distinguish it from other variants of the same product.

**Monitoring center:** Designated location where offender tracking data are received and alerts are responded to (in accordance with the protocol established by the agency).

**Multi-channel receiver:** Simultaneously tracks more than one satellite signal.

**Multi-plexing channel:** Sequenced through a number of satellite signals.

**Multi-path error:** Caused by the interference of a signal that has reached the receiver antenna by two or more different routes. Usually caused by one path being bounced or reflected.

**Multi-piece system:** OTS configuration that consists of, at a minimum, both body-worn and body-attached components.
National Information Exchange Model (NIEM): A collaborative (public/private), XML-based framework designed to develop, disseminate and support enterprise-wide standards and processes that will enable jurisdictions to automate information sharing.

Near real time: Refers to the delay introduced, for electronic communication and automated data processing, between the occurrence of an event and the delivery of the processed data, and implies that there are no significant delays.

New unit/New device: Contains all original parts and has not previously been shipped from the manufacturing location to any user agency.

Notification: Process of advising the subscribing agency of selected events.

Offender tracking: Process of continuously monitoring the location of an individual, using a location-based service.

Optimal conditions: Generally a testing environment free of precipitation that has no obstructions extending higher than 15 degrees above the horizon.

OTS hardware: Tracking device and peripheral equipment assigned and provided to a participant as part of his/her enrollment in an offender tracking program.

OTS software: Various computer programs used to direct the operations of an OTS, especially as it relates to the interface with the end user. These programs may exist within the tracking devices themselves (firmware) or within the manufacturer’s computer systems, and may also be resident on computers controlled by the end user.

Offender tracking system (OTS): Technology, consisting of hardware and software segments, designed to determine and report at programmed intervals the geographic location of a person (a participant) who is subject to criminal justice system supervision.

OTS manufacturer: Commercial enterprise engaged in the design and/or fabrication of a product model submitted for certification.

On-board processing: Approach to location data analysis that compares dynamic location data to static zone data stored in memory on the offender-worn device to determine whether a zone alert should be generated and communicated.

One-piece device: Body-attached offender tracking component that can acquire and record location information without using a separate tethering device.

Open-air environment: Taking place in, or characteristic of, a setting in which no obstructions extend higher than 15 degrees above the horizon.
Outlier: Tracking location point that reflects improbable participant motion and appears as a “spike” when displayed graphically with location points that immediately precede and follow the outlier. Often attributable to multi-path error (see above).

P-code: Precise or protected code. A very long sequence of pseudo-random binary biphase modulations on the GPS carrier at a chip rate of 10.23 MHz, which repeats about every 267 days. Each one-week segment of this code is unique to one GPS satellite and is reset each week.

Participant: Person subject to criminal justice system supervision who is wearing, or is assigned to wear, an OTS hardware unit in connection with that supervision.

Passive tracking: Approach in which device location and status data are stored in device memory and transmitted retrospectively. Data may be transmitted at fixed intervals using cellular capability, or may be transmitted when the device is connected to a telephone line.

Percent dilution of position (PDOP): Measure of the geometrical strength of the GPS satellite configuration or the amount of error in a position. A PDOP value of less than four indicates the best accuracy (under one meter). A value of between four and eight indicates acceptable accuracy. A value of greater than eight indicates poor accuracy.

Point: See Location point.

Portable communications device: Handheld or wearable unit that provides the user with mobile communication and/or computing capability (e.g., cellular telephone, personal digital assistant, pager, smartphone, tablet).

Post-processing: Approach to location data analysis that compares dynamic location data to static zone data stored on a server to determine whether a zone alert should be generated and communicated. Post-processing generally is used when the number of zones applicable to an offender precludes on-board processing of dynamic location data.

Post-processed differential GPS: Base and roving receivers with no active data link between them each record the satellite observations that will allow differential correction at a later time. Differential correction software is used to combine and process the data collected from these receivers.

Precision algorithm: Mathematical rectification model used to improve the positioning accuracy of an OTS device.

Prime meridian: Line of longitude that runs through Greenwich, United Kingdom, and is used as the origin for longitudinal measurements.

Product: One unit of a specific OTS model.
Product label: Marking affixed by an OTS manufacturer to each unit of a compliant model that contains required product and model information and the mark of conformity to standards.

Proximity tamper: Alert that occurs when the distance between the body-attached portion of a tracking device and the portion of the body to which it is attached exceeds a predetermined value.

Pseudo-lite: A ground-based differential GPS receiver that transmits a signal like that of an actual GPS satellite, and can be used for ranging.

Refurbished unit/device: (1) Provided by the OTS manufacturer to a user agency after modification by replacement of system-level components, including the casing and excluding straps and field-replaceable batteries, with identical components and assignment of a modified serial number. (2) Manufactured from used system-level components and assigned a unique serial number with the intent to provide it to a user agency.

Relative accuracy: Difference between how features on a map and those same features in the real world are positioned in relationship to each other. A measurement system may employ a bias or systematic error, with consequently inaccurate results, but still preserve local relationships.

Removal: Detachment of a body-attached OTS unit from a participant.

Repaired product: OTS unit submitted to the OTS manufacturer for correction of a defect, failure or functional issue, and that, after correction, is returned to the submitting user agency without change to the unit’s serial number.

Resolution: Minimum distance that can be recorded by a measurement system. For example, if a map has a resolution of 10 meters, the map cannot accurately depict features smaller than 10 meters. Therefore, these features may be depicted as points, or they may not be depicted at all.

Reverse geocoding: Process of determining associated textual data, such as street addresses or postal codes, from geographic coordinates.

Satellite elevation mask: Required elevation of the GPS satellite above the horizon. Satellites with elevation below the mask will not be used to compute positions. This is done because satellites near the horizon have more error due to atmosphere.

Satellite view: See aerial view.

Selective availability (SA): Errors in data and satellite-clock dithering deliberately induced by the U.S. Department of Defense to restrict full GPS accuracy to authorized users, typically the U.S. military.
Serial number: Unique alphanumeric identifier applied by an OTS manufacturer to each unit of a particular product model that distinguishes it from every other unit of that product model produced by the OTS manufacturer.

Shielding: Intentional application of an object or substance, usually metallic, to the exterior of an OTS device for the purpose of blocking incoming and/or outgoing radio signals.

Shock: Transmission of kinetic energy into a tracking device, usually by dropping (collision with a stationary object) or impact (collision with a moving object).

Signal-to-noise ratio (SNR): Measure of the relative ratio of information content. A higher number is desirable.

Spoofing: Circumvention technique that attempts to deceive the OTS by providing false device or location data to the tracking device for communication to the OTS.

Strap tamper: Alert generated when a body-attached device detects that the method of attaching the device, including its components, has been cut or otherwise compromised to the point that removal of a body-attached device could occur.

System-level components: Key parts of an OTS model that, when certified, cannot be changed or modified without first receiving the authorization of the Certification Body. These items include any casings, antennas, communication devices, batteries, straps/attachment pins or devices, transmitters/receivers and indicators to the participant. Any of these components present in the body-attached portion of multi-piece configurations are also considered system level components.

System log: Compilation of time-stamped and reportable events generated by an OTS.

Tamper: Event in which there is an attempted or completed effort by a participant to disrupt or disable the monitoring or communications of his/her tracking device.

Tamper evident: Design or manufacturing process that makes participant attempts to tamper with device components easily detectable by leaving physical evidence.

Tether/tethering device: Common reference to the body-attached portion of a multi-piece tracking system.

Tether gone: Event in which the tether and tracking device of a multi-piece OTS are separated by a specified distance for a predetermined length of time.

Time to first fix (TTFF): Specification related to the interval required for a GPS receiver to acquire GPS satellite signals and navigation data, and to calculate the receiver’s position. TTFF specifications generally are expressed with reference to the receiver’s operating condition: cold, warm or hot (see cold start, warm start and hot start).
Trilateration: Position location methodology that calculates location by measuring the time difference of arrival of signals from three or more transmitters at known locations.

Two-piece device: (See multi-piece system).

Uninterruptible power supply: Electrical device used to provide auxiliary capacity in the event of loss of main capacity.

Unit: One item of a particular OTS hardware product model.

Used unit: An OTS device that contains all of its original system-level components, excluding straps and field-replaceable batteries, and that was previously shipped from the manufacturer to a user agency. As it has not been modified, it maintains its original serial number.

Vendor: A seller or reseller of offender tracking systems.

Vibration: A rapid linear motion of a particle or of an elastic solid about an equilibrium position.

Violation: An alert event defined by an agency as an infraction of its program rules.

Warm start: Operational condition of a GPS receiver when the receiver has relatively accurate estimates of the current time, the position and velocity of the receiver, and valid satellite location data.

Water-resistant: Construction designed to resist the ingress of water into a device.

Watertight: Construction designed to be impermeable to water, except when under sufficient pressure to produce structural discontinuity.

Wi-Fi: Registered trademark of the Wi-Fi Alliance, denotes conformity to the IEEE 802.11 standard of interoperability. In common use, the term refers generally to technology, based on the IEEE 802.11 standard, that uses wireless connectivity.

Zone: User-defined geographic area intended to restrict the movement of a participant during specified periods and to trigger notification to the user agency if the area boundaries are traversed by a participant to whom the zone applies.

Zone template: Overlay, or pattern, containing multiple areas of specified types that an agency may create once and apply as needed to multiple participants.
Appendix B: Links and Reference Materials

Electronic Monitoring Resource Center
The National Institute of Justice Center of Excellence for Corrections Technology, part of the National Law Enforcement and Corrections Technology Center System, developed the Electronic Monitoring Resource Center (EMRC) to serve as a clearinghouse for hundreds of articles and research papers related to all aspects of electronic monitoring. The STC relied heavily on material from the EMRC in the development of this document and of the Offender Tracking Standard as a whole. Law enforcement and corrections employees working in this field should register with EMRC to have access to this wealth of information concerning offender monitoring.

https://emresourcecenter.nlectc.du.edu/

Contact Allergen Database
The Contact Allergen Database provides information on the more common causes of allergic contact dermatitis.

This is a private website and the information is provided as educational only and is not intended to substitute for medical care or recommendations by a physician.

http://contactallergy.com/

Offender Supervision With Electronic Technology: A User’s Guide
Prepared by the American Probation and Parole Association (APPA) with NIJ funding, this 2002 document helps readers understand and appreciate the process needed to incorporate and implement electronic supervision strategies within justice system programs. It was developed for agency staff who want either to introduce electronic supervision as a new program component or enhance the use of electronic supervision that has already been implemented. The document is divided into five sections:

- Developing or Enhanced the Use of Electronic Supervision Tools.
- Obtaining and Maintaining Needed Resources.
- Supervising Offenders With Electronic Technologies.
- Program Accountability.

Offender Supervision With Electronic Technology (second edition)

This publication updates *Offender Supervision With Electronic Technology: A User’s Guide.* Prepared by APPA with funding from the Bureau of Justice Assistance, this 2009 document was developed with an emphasis on GPS technology and offender tracking applications as well as the relationship between electronic supervision and evidence based practices.


Global Positioning System (GPS) Technology for Community Supervision: Lessons Learned

Prepared by Noblis through an award from NIJ, this 2007 publication documents the kinds of success and challenges that supervision agencies face when using GPS to track clients. This report is the result of interviews with seven community supervision agencies about their experiences using GPS to manage clients. The study also researched GPS and other location-based tracking technologies as well as GPS standards and evaluations of GPS programs. It is the intention of this report to provide information to practitioners and other stakeholders at every jurisdictional level that will help them to better understand the use of GPS in community supervision.

[https://www.ncjrs.gov/pdffiles1/nij/grants/219376.pdf](https://www.ncjrs.gov/pdffiles1/nij/grants/219376.pdf)
Appendix C: Offender Tracking System Project Rosters

This document was developed by a Special Technical Committee of practitioners, technical experts, and others with experience in standards development and conformity assessment.

Contributors:

STC members (To be listed upon completion)

NIJ (To be listed upon completion)

Advisory Working Group:

AWG members (To be listed upon completion)