COMMERCIALIZATION OFFICE - PILOT OPERATIONAL REQUIREMENTS DOCUMENT

Integrated Intrusion Protection (IIP)

February 2009

Point of Contact:

Mark Protacio
DHS S&T Commercialization Office
SETA Support
Mark.Protacio@associates.dhs.gov

Contents

1. General Description of Operational Capability

Currently, the overall surveillance function for the Department of Homeland Security (DHS) is performed using a variety of technologies including video, infrared, sound, pressure and vibration sensing. Each of these solutions, with its advantages and vulnerabilities, is useful for a narrow range of specific surveillance needs. However, the need exists for an adaptable, scalable surveillance capability that provides automated, real-time protection for a wide range of operational scenarios. DHS must also be able to leverage use of non-real-time intelligence data associated with any suspicious activity or perceived preparations prior to a critical event. In addition, the full cadre of surveillance delivery systems must be considered. An integrated intrusion protection (IIP) system is necessary.

This advanced capability must effectively support different types of protection without the need for 24/7 staffing. It must also be simple and quick to deploy, effective for a variety of surveillance area types, sizes and require little maintenance. Finally, it must be cost-effective to use, even for temporary protection needs. This capability is useful to missions performed by the DHS National Protection and Programs Directorate (NPPD) (specifically the Office of Infrastructure Protection), the Transportation Security Administration (TSA), the U.S. Customs and Border Protection (CBP), the U.S. Coast Guard, and the Federal Emergency Management Agency (FEMA), as well as critical infrastructure/key resources (CI/KR) owners and operators and first responders.

1.1. Capability Gap

Current surveillance technology does not adequately address the variety of surveillance needs. For example, most surveillance systems, including video surveillance, require major investments in time, materials and staffing to deploy. Additionally, a video surveillance system requires thorough planning for effective installation to overcome its normally limited coverage area, requires constant monitor staffing and is usually costly due to technology, installation and maintenance costs. After a major disaster, for example, FEMA must establish surveillance of geographic areas very rapidly and with minimum overhead for multiple reasons. For instance, if a post-disaster neighborhood presents critical, life-threatening hazards that were not present prior to the disaster, FEMA may decide to prohibit unauthorized personnel from entering the area until it is secured. In order to enforce this, surveillance of the area may need to be established to notify authorities if an intruder enters. The same paradigm applies when a user must keep an area from being looted after a disaster. A rapidly deployable, wide-area surveillance system is necessary to meet these needs.

Another example includes supplies that are forward-deployed in preparation for a disaster. These supplies require protection from theft or sabotage. Ideally, a surveillance system to protect these supplies would provide sufficient warning to apprehend or deter the intruder before a theft or sabotage occurs. However, if these supplies are stored in existing commercial storage units next to a street with frequent foot and vehicular traffic, a surveillance perimeter large enough to provide such warning may be impractical. Therefore, security may arrive on site after the intruder has departed. Information to characterize an intrusion, such as whether the intruder was on foot or not and/or whether the intruder removed supplies or left an object behind to commit an act of sabotage is useful to arriving security forces. Such a system would need to cover the site internally and externally and be staffed persistently. In this case, an adaptable and automated surveillance capability that provides intrusion characterization to security forces after the actual intrusion may be more cost-effective.

As previously mentioned, this capability gap is not confined to FEMA alone. For example, a critical requirement for the Office of Infrastructure Protection is protection surveillance for critical infrastructure; such as a dam that provides power or water for a major urban area. Access to a dam often involves rough terrain and a wide geographic area. Traditional surveillance technology such as video, infrared, pressure and sound sensors do not usually cover large areas of rough terrain effectively. In addition, to maximize protection, surveillance must detect an intruder early enough to enable security to prevent the intruder from reaching the dam. Therefore, the traditional solution is often security patrols. Such random patrols are costly, labor intensive and require training of patrol personnel. Patrol vehicles require a major investment and regular, costly maintenance. An automated, real-time, readily deployable, wide-area surveillance system is more persistent, cost-effective and would make better use of limited security personnel.

1.2. Overall Mission Area Description

The IIP system shall address infrastructure protection and incident management mission needs. It shall be used to protect national and local infrastructure, storage facilities and geographic areas when benign intrusion does not frequently occur unexpectedly, i.e., authorized personnel do not regularly enter the surveillance area without notification. Therefore, IIP users shall primarily be first responders and security personnel at the national, state, local or tribal levels.

An IIP system shall provide rapidly deployable and reliable surveillance over large geographic areas. It may effectively detect intruders sufficiently early for authorized personnel to intercept them prior to an intruder penetrating the target or may be used to detect changes to the protected area when intruders cannot be prevented from reaching the site. In addition, the IIP system shall characterize (time, location, type) the intrusion to enable alarms and an appropriate security response. Finally, an IIP shall provide different types of automated alarms so that security personnel are notified and involved only when needed. For instance, an IIP system may be configured to provide warnings when a suspicious person is walking toward the protected area and an alarm when that person has become an intruder by entering the protected area. The system does not require around-the-clock staffing to monitor the surveillance area.

1.3. Description of the Proposed Product or System

The IIP system shall be composed of the following major subsystems:

1. A sensor array
2. One or more sensor signal receivers
3. A central processor
4. A communication system

Whenever possible, the sensors shall be COTS products. These sensor arrays shall be distributable around the protection perimeter and any specific areas of interest, such as a road, or the geographic area to be monitored. In addition, these sensor arrays may be fastened to walls of storage units to sense reductions or additions to the unit contents.

The sensor signal receiver(s) shall be composed of COTS products. These receivers shall either receive signals sent from the sensors or interrogate sensors for a response. Mobile sensors may be deployed to supplement permanently deployed sensors, if required.

A “sensor fusion” processor shall also be a COTS product. This processor shall be used to define a characteristic surveillance baseline and representative intruder responses from a sensor set. As responses are received from the sensor signal receivers, the processor shall match these responses with characteristic baseline and intruder responses. If a response matches the baseline within defined thresholds, the processor shall simply wait for the next signal set. If the response matches an intruder within defined thresholds, the processor shall notify security via the communication system of that intrusion type. Intrusion types include, for example, one or more intruders on foot or vehicles. An anomalous response type shall also be defined to alert security of uncharacterized intrusions, other surveillance area changes (e.g., a tree falling in the woods is heard) or IIP equipment failures.

1.4. Supporting Analysis

These capability gaps have been verified through interviews with DHS, CI/KR and first responder personnel throughout the United States.

1.5. Mission the Proposed System Shall Accomplish

The IIP system shall provide an easily deployable, adaptable and low maintenance solution for the surveillance of various geographic areas related to actions of harmful or illegal intent. It shall provide reliable, effective detection of intruders and characterize them according to pre-defined intrusion categories. Dependent on the protection level required and site specifics, this automated intrusion detection system may establish a perimeter to provide sufficient lead time for authorized personnel to intercept the intruder before the target area is breached. The IIP system shall also determine if the intruder removed or left something at the site and where it was placed. The IIP system shall be cost-effective and most, if not all, of its components may be re-used for subsequent surveillance deployments. It shall be capable to use as a stand-alone surveillance system or may be easily integrated with additional surveillance technologies.

1.6. Operational and Support Concept

1.6.1. Concept of Operations

IIP is intended as a surveillance system in a “security toolbox.” It has the advantages of:

1. Providing surveillance of large areas
2. Characterizing intrusions for authorized responders
3. Providing early intrusion warnings
4. Responding automatically, so that continuous staffing is not required
5. Being rapidly deployable with minimal planning for various terrains
6. Being adaptable to different surveillance areas
7. Requiring little training to deploy and operate
8. Requiring minimal maintenance
9. Using COTS technology
10. Providing cueing to other security systems such as video systems, once an intrusion has been detected

The IIP system most effectively protects areas that are typically low density in terms of human and vehicle operations. If supply storage or infrastructure is situated near a busy footpath, street or highway on a small plot, other surveillance methods may be more appropriate for protection from intruders at the current time. For example, many public storage facilities are near busy streets, and during the daytime, high-profile public sites such as the Washington Monument are constantly surrounded by tourists.

The current low density constraint is due to the need to control false alarms. For instance, if a supply storage facility is located near a busy street, each pedestrian and passing vehicle may interact with the sensor array, causing an atypical response, and thus notifying security of a possible intruder. However, if the supply storage facility is separated from nearby traffic by some distance, IIP could be an appropriate solution. We are interested in solutions that minimize false alarms with high foot or vehicular traffic.

The IIP deployment attributes listed above make it ideal for situations requiring rapid deployment (e.g. during emergencies and disasters). For example, an agency may decide to deploy IIP for multiple scenario classes. One would be to protect forward-deployed supply storage. In the event of a potential emergency such as an impending hurricane, one may decide to pre-deploy supplies to reduce the loss of life and property in the event of hurricane impact. In addition, after a disaster has occurred officials may also determine that specific geographic areas must be protected. For instance, one may decide to deny access to areas that have become hazardous or are potential looting sites.

Another application may be to choose to deploy IIP over large geographic areas to protect critical national infrastructure. Such infrastructure includes defense industrial bases; energy; national monuments and icons; dams; commercial nuclear reactors, materials, and waste; telecommunications; transportation systems; and other government facilities.

In each case, sensors may be deployed by distributing them around the perimeter of the area to be protected and areas of special interest such as access roads. If intruders are to be intercepted by security prior to reaching the protected site, planning is required to determine the perimeter distance from the target to assure adequate response time. If interception is not required, the perimeter may be deployed around a smaller area. If a stealth configuration is desired, sensors shall be able to be easily hidden or camouflaged. These sensors may also be fastened to the protected site itself if there is a concern for sabotage or a desire to learn if something has been removed from a storage building.

Sensor signal receiver(s) are installed within range of the sensors. Since the sensor signal receiver(s) may be connected to the processor by either wireless or internet cable, the processor may be located at the protected site, at the local security site, or anywhere with network connectivity. When the sensors have been distributed, the sensor signal receiver(s) responses are processed by the processor to define a “baseline” response pattern. This process calibrates the IIP to recognize a nominal, non-intrusion state.

Over time, most sites shall undergo changes. To accommodate such changes, the processor shall provide the option to “reset” the baseline either manually or at preset intervals. The processor enables IIP to be self-learning based on updated information and disposition of the area of interest. The system shall go through a calibration sequence each time “reset” is initiated in order to establish a new baseline. After the baseline has been established, the system responses to intrusion types of interest are also defined if desired. System responses to each intruder type are characterized using actual intruder approaches and entrances of the IIP surveillance area.

As IIP operates, each time a non-baseline state (including unlawful intrusions) is identified, the system response information is recorded. Intrusion and non-baseline state information may be retrieved from the processor using a standard network interface.

1.6.2. Support Concept

An IIP system shall be designed to require minimal maintenance. All sensors and detection array pieces shall be extremely rugged and produced to withstand extreme temperatures and physical changes. These sensor products need to be optimized for use under a wide range of environmental conditions and may be fastened or placed on almost any surface. If one of these sensors fails operationally, this shall be reflected as an anomalous condition by the processor. As the replacement of a failed sensor power unit is the primary IIP maintenance required, sensor batteries are the only significant spares required.

System function is regularly reported to security if the system response is nominal, thereby automatically testing system function and communications. Diagnostics for the IIP-specific components shall be built-in and may be executed automatically. Baseline response recalibration may also be configured to be executed automatically after a specified interval or may be performed manually as necessary.

2. Threat

Intruders may be civilians returning to the scene of a disaster, looters, saboteurs, or potentially international/domestic terrorists.

The evidence for people returning to hazardous disaster areas is well documented. People return for a variety of reasons, such as searching for a relative or pet or to retrieve a possession. These people put themselves, and potentially rescue workers in harm’s way. Hazards include the remains of buildings after collapsing during an earthquake, wild animals after a flood, contagions after a hurricane, or poisonous chemical exposure after a terrorist attack. Intruders create a health hazard that may result in the loss of life.

The evidence for looters invading a disaster area is also well documented. Looters rob from unattended sites, including disaster sites as well as unattended supply storage units. Their methods often result in property damage as well as theft of property. In addition, they create a situation in which the risk of injury or loss of life to themselves and to the other people present is dramatically increased. These risks result from their looting methods or conflicts resulting from such looting. Saboteurs and terrorists may attack infrastructure or intrude disaster sites. They may intrude disaster areas to create the potential for further disaster. These means may include chemical or biological agents that may be more vulnerable to theft, during or after a disaster.

3. Existing System Shortfalls

Existing systems do provide effective intrusion detection within range of their sensors. For infrared (IR), this range is extremely short as background IR energy overcomes the source energy. Sound also suffers from the same range limitations and is problematic in an outdoor setting. For video, the effective range is limited by the need for an identifiable image. Although video sensor coverage area may be increased by the use of wide angle lenses, the range of an identifiable image diminishes rapidly as the lens angle increases. Many current solutions also store collected data to be retrieved only after an event occurs. This may help identify the culprit, but not prevent the disaster. None of these systems automatically detects how an intruder may have changed the protected site, e.g., placed something at the site such as a bomb or removed something from the site. It is essential that surveillance data be collected and processed prior to and during potential suspicious events.

Therefore, traditional surveillance sensor types are inadequate to cover diverse geographic areas without the added (and often prohibitive) expense of planning and the installation of large numbers of costly sensors. Deployment of each of these systems requires expert analysis of the coverage area due to their small, interactive coverage areas. In addition, if sufficient warning time for security response is required, these sensor types may have to be installed in multiple layers, at a minimum with a warning layer and an actual intrusion layer. Each technology requires significant time to deploy and test. Operation of sound and infrared systems may provide cost-effective automatic detection for limited range. Video may provide automatic detection, but is prone to spoofing and costs much more than the same capability for sound or infrared systems. Therefore, operations for video systems are costly due to the need for continuous staffing during the threat period as well as the expense of the technology. Substantial training is required to deploy and maintain video systems. Further, video systems require regular maintenance due to scanning platforms and the need to clean the lenses of outdoor systems. Sound and infrared systems are much cheaper to operate and maintain due to their automatic capability and the cost of the technology.

In summary, infrared and sound systems provide limited coverage but tend to be cost-effective. Video systems provide intrusion identification, have larger coverage areas, yet tend to be costly to deploy, operate and maintain.

4. Capabilities Required

4.1. Operational Performance Parameters

Operational Performance parameters are labeled as either Threshold (T) or Objective (O). Threshold parameters are the minimum parameters to be met for system utility. Objective parameters are the desired values for system operation. If a parameter is marked without a T or O indicator, it is an Objective parameter.

4.1.1. Effective Intrusion detection

The IIP system shall provide the capability to detect 98% (T)/ 99.9% (O) of defined intrusions within a defined protected area.

The IIP system shall provide the capability to read data from each sensor in real-time.

The IIP system shall provide the capability to locate intrusions to ≤ 20 meters (T)/ ≤ 3 meters (O) of their true location. Location accuracy is dependent on sensor placement.

4.1.2. False Alarm rate

The IIP system shall generate ≤ 0.1% (T)/ ≤ 0.01% (O) false alarms.

4.1.3. Intruder characterization

The IIP system shall provide the capability to identify intrusions by human beings, animals, vehicles and/or robots.

4.1.4. Real-time intruder information

The IIP system shall provide the capability to send real-time intruder warning messages to security. "Warning" messages are sent when intruders approach (i.e., before they enter) the coverage area.

The IIP system shall provide the capability to send real-time intruder alarm messages to security. "Alarm" messages are sent when intruders penetrate the coverage area.

The IIP system shall provide the capability to send real-time updates of intruder information to investigating security personnel.

4.1.5. Intrusion Site Change Characterization

The IIP system shall provide the capability to detect changes to the protected site. These changes include 1) adding something, 2) removing something, or 3) physically changing the site in a pre-set limit involving minimal size and weight, and the type of object. Please specify the size, weight and type of object specifications.

4.1.6. Automated Operation

The IIP system shall provide the capability to continuously monitor a defined area automatically.

The IIP system shall provide the capability to identify intrusions (see 4.1.5) automatically.

The IIP system shall provide the capability to send multiple intrusion alarm levels automatically.

4.1.7. Highly Adaptable Surveillance Coverage

The IIP system shall provide the capability to provide effective surveillance for any area with sensors deployed by less than their maximum range.

4.1.8. Sensors

The IIP system sensors shall operate normally in temperate ranges from ≥ 140°F (60°C) to ≤ - 35°F (-37°C).

4.1.9. Sensor signal receivers

The IIP system sensor signal receiver shall normally receive sensor data from a range of ≥ 100 meters (T)/ ≥ 1 kilometer (O).

4.2. Key Performance Parameters (KPPs)

4.2.1. Cost-Effectiveness

The IIP system kit shall provide surveillance of at least 10,000 square meters for ≤ $8,000 (in volume production quantities). Additional kits may be combined to monitor larger coverage areas.

4.2.2. Deployment Schedule

The IIP system shall provide the capability to deploy, configure and test an area of ≥ 10,000 square meters in surveillance coverage, with operational status within 24 hours.

4.2.3. Maximum Coverage Area

The IIP system shall provide surveillance coverage capability of any size area. Larger areas shall require additional sensors and sensor signal receivers, or their equivalent.

4.3 System Performance.

4.3.1 Mission Scenarios

Two primary scenarios were posited in the operations concepts section: 1) a pre-disaster deployment to protect forward-deployed supply storage and 2) a post-disaster deployment to deny access to areas that have become hazardous or are potential looting sites. The IIP system may also be deployed to provide surveillance for large geographic areas necessary to protect critical national infrastructure.

4.3.2 System Performance Parameters

4.3.2.1. Sensors

All IIP system sensors shall be COTS products (T).

All IIP system sensors shall operate continuously using self-contained power for a minimum ≥ 6 months (T)/ ≥ 24 months (O).

4.3.2.2. Sensor signal receivers

The IIP system sensor signal receiver shall be composed of COTS hardware (T).

The IIP system sensor signal receiver software shall execute on a COTS lower-cost personal computer (T).

4.3.2.3 “Sensor fusion” processor

The IIP system processor shall be composed of COTS hardware (T).

All IIP system software shall execute on a COTS personal computer (T).

The IIP system processor shall be capable of storing intrusion data for ≥ 3 months (T)/ ≥ 6 months (O).

4.3.3 Interoperability

The IIP system processor shall be capable of communication using a hardwired or wireless network, using standard TCP/IP protocols.

4.3.4 Human Interface Requirements

The IIP system human interface shall comply with Windows GUI standards. The processor shall provide the human interface to the entire system including the configuration and diagnostics for the sensor signal receiver.

4.3.5 Logistics and Readiness

The system shall be operational for long periods of continuous operation without interruption. Independent of individual sensor failures, the mean time between failure (MTBF) shall be ≥ 5,000 hours (T)/ ≥ 25,000 hours (O).

4.3.6 Other System Characteristics

The system shall be designed for 1) unattended and automatic operation, 2) rapid deployment, 3) low maintenance, 4) use of low cost components, 5) use of easily replaceable components, 6) use of readily available components, 7) rapid, simple deployment, 8) deployment by staff with little or no prior training, 9) operation by staff with little or no prior training, and 10) maintenance by staff with little or no prior training.

5. System Support

5.1 Maintenance

Each IIP system shall provide both visual and auditory indications of system anomalies. Diagnostics may be executed automatically or manually from the processor user interface. Manual execution requires minimal training. The processor user interface shall provide user access to diagnostic results.

Diagnostics shall identify IIP subsystems that require maintenance including sensors that require consumable replacement. Replacement of specific sensors or sensor batteries/other consumables shall be performed by personnel with minimal or no training. Other maintenance shall be performed by replacing the subsystem.

5.2 Supply

No special tools or support equipment shall be required for deployment or subsystem replacement. Manuals shall be provided to the operator by the vendor and shall include deployment procedures, information on diagnostic indicators (both automatic and manual diagnostics) and replacement procedures. The manuals shall also provide information on system data retrieval.

5.3 Support Equipment

All diagnostics shall be provided by the system. No external support equipment shall be required for the operator to maintain and operate the system.

5.4 Training

Users shall be instructed on the deployment, operation, and routine maintenance of system, interpretation of diagnostic indicators (both automatic and manual) and data retrieval procedures. In addition, manuals and written procedures supplied by the system developer shall be of sufficient detail to enable the execution of each of these activities by untrained personnel.

5.5 Transportation and Facilities

Transportation of IIP system components is expected and shall be well within individual carriage limitations for standard automobiles. Sensor equipment shall be small and light, and the sensor signal receivers and processor shall be no larger than the size of a desktop computer. The needs for cables, wires, etc, for most installations shall be minimal.

Once deployed, IIP system components shall remain in place until removed or replaced. The number of sensors required shall depend on the surveillance coverage area size, shape, terrain and existing access among other factors.

Transportation of retrieved digital media shall require no special technical capability but should be conducted consistent with applicable procedures to preserve chain of custody when data retrieval is conducted for use in legal proceedings (e.g. criminal prosecution or civil litigation).

Facilities for housing the sensor signal receiver(s) and the processor shall require standard 110 V 60 Hz AC and protection from the elements. Fixed buildings, mobile units and tents shall suffice, given the other requirements.

6. Force Structure

Each IIP system deployment can be unique, dependent on the protection mission and the geographical coverage area. For instance, the value of the protected infrastructure shall determine the distance of the protection perimeter from this target, the depth of the perimeter and the density of sensors deployed within the perimeter. The required security response time shall define the distance of the perimeter from the target.

Sensor placement is dependent on a number of factors. The complexity of existing access to the target shall guide additional sensor placement to monitor this access and the areas around this access. The coverage area shall dictate sensor placement as its size, shape and terrain shall determine the number of sensors and how they are to be deployed. Finally, the sensor type shall establish deployment choices. The sensor type, active or passive (simple transponders), shall determine sensor transmission range and maintenance schedule. Sensors may be placed outdoors on a solid surface or may be shallowly buried. Sensors may also be mounted on vertical or overhead surfaces to achieve specific surveillance requirements. Sensors may not be submerged underwater.

Sensor signal receiver(s) shall be deployed based on sensor signal receiver type (how many sensors may be processed by the type), the number of sensors deployed, and the range limits of

the sensors and the receiver. Sensor signal receivers shall require protection from the elements and standard 110 V 60 Hz AC power. Sensor signal receivers shall require cable or wireless network access to the processor, but are not required to be co-located with it. A single processor shall be deployed to process data from each of the deployed sensor signal receivers. It shall require protection from the elements and standard 110 V 60 Hz AC power. It shall also require cable or wireless network access to the sensor signal receivers. Assuming a communications infrastructure is accessible and readily available; it shall require duplex access to security forces via cable or wireless network, telephone, or radio.

7. Schedule

An operational capability shall be defined as the demonstration of enough deployed sensors to monitor at least a 10,000 square meter area, the necessary sensor signal receiver(s) and a processor (or equivalent signal processing equipment) within one year.

8. System Affordability

The price of an IIP system kit shall be ≤ $8,000 based on high volume production. This price shall include the software, hardware and documentation to deploy, operate and maintain the system kit. The system kit components include: 1) sufficient sensors to cover an area of at least 10,000 square meters, 2) sufficient receiving and processing equipment to monitor the sensor array, and 3) software on compact disc for installation on computers as required.

The price is all inclusive. No special consulting fees/services for the system kit are permitted for any scenario the vendor accepts.