DEPARTMENT OF HOMELAND SECURITY

Office of Inspector General

A Review of Remote Surveillance Technology Along U.S. Land Borders

Office of Inspections and Special Reviews

OIG-06-15

December 2005

Office of Inspector General

U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

Preface

The Department of Homeland Security (DHS) Office of Inspector General (OIG) was established by the *Homeland Security Act of 2002* (Public Law 107-296) by amendment to the *Inspector General Act of 1978*. This is one of a series of audit, inspection, and special reports prepared as part of our oversight responsibility to promote economy, effectiveness, and efficiency within the department.

This report evaluates the effectiveness of border surveillance, remote assessment, and monitoring technology in assisting the Bureau of Customs and Border Protection (CBP) to detect illegal entry into the United States. It is based on interviews with employees and officials of relevant agencies and institutions, direct observations, statistical analyses, and a review of applicable documents.

The recommendations herein have been developed to the best knowledge available to our office, and have been discussed in draft with those responsible for implementation. It is our hope that this report will result in more effective, efficient, and economical operations. We express our appreciation to all of those who contributed to the preparation of this report.

Richard L. Skinner
Inspector General

Table of Contents

Figures

Appendices

Abbreviations

ASI	America's Shield Initiative
BPA	Blanket Purchase Agreement
BTS	Border and Transportation Security Directorate
CBP	Customs and Border Protection
CLIN	Contract Line Item Number
DHS	Department of Homeland Security
FAA	Federal Aviation Administration
FY	Fiscal Year
GAO	Government Accountability Office
GSA	General Services Administration
ICAD	Intelligent Computer Assisted Detection
IMC	International Microwave Corporation
INS	Immigration and Naturalization Service
ISIS	Integrated Surveillance Intelligence System
IT	Information Technology
LECA	Law Enforcement Communication Assistant
MOU	Memorandum of Understanding
NAS	National Airspace System
NEPA	National Environmental Policy Act
OBP	Office of Border Patrol
OIG	Office of Inspector General
OIRM	Office of Information Resources Management
OIT	Office of Information Technology
PMC	Performance Management Consulting
POE	Port of Entry
PPB	Office of Plans, Programs and Budget
RVS	Remote Video Surveillance
S&T	Science and Technology Directorate
TD	Technical Directive / Task Directive
UAV	Unmanned Aerial Vehicle
USACE	U.S. Army Corps of Engineers

Executive Summary

The Office of Border Patrol (OBP), within the Department of Homeland Security's (DHS) Bureau of Customs and Border Protection (CBP), is the primary federal law enforcement organization responsible for detecting and preventing illegal aliens, terrorists, and contraband from entering the United States between official ports of entry (POEs). To help accomplish its mission, OBP uses technology, including cameras and sensors, to detect and identify illegal border intrusions. Cameras - both daylight and thermal-infrared, installed on poles and other structures along high volume illegal alien traffic areas of the border - constitute the Remote Video Surveillance (RVS) system. Sensors are also used along high volume illegal alien traffic areas of the border.

Remote surveillance technology is managed by OBP under the auspices of the Integrated Surveillance Intelligence System (ISIS) program and the America's Shield Initiative (ASI). The ISIS program and ASI have received funding annually since Fiscal Year (FY) 1997 -- to date more than $429 million.[1] Several limitations of border surveillance and remote assessment and monitoring technology as well as significant delays and cost overruns in the procurement of the RVS system have impeded the success of ISIS.

- ISIS components are not fully integrated, e.g., when a sensor is activated, a camera does not automatically pan in the direction of the activated sensor. In addition, RVS cameras do not have detection capability regardless of whether they are used in conjunction with sensors. To complicate matters further, because current sensors cannot differentiate between illegal alien activity and incidental activations, caused by animals, seismic activity, or weather, OBP agents are often dispatched to false alarms.

[1] The ISIS program was initiated while the Border Patrol was part of the Department of Justice's Immigration and Naturalization Service (INS). Within INS, the Office of Information Resources Management (OIRM) was the principal manager of the ISIS program. In April 2001, a memorandum of understanding was established between OIRM and Border Patrol that transferred the RVS system and sensor program to Border Patrol and left the Integrated Computer Assisted Detection (ICAD) component of ISIS with OIRM. When Border Patrol was brought under DHS in March 2003, all ISIS elements transferred to the Border Patrol. All references to OBP refer to both current and legacy INS activities related to the ISIS program.

- OBP was unable to quantify force-multiplication benefits of remote surveillance technology. Further, data entered into OBP's primary source of ISIS information, the ICAD system, is incomplete and not consistently recorded by OBP sectors.

- Based on an analysis of sample ICAD data, ISIS remote surveillance technology yielded few apprehensions as a percentage of detection, resulted in needless investigations of legitimate activity, and consumed valuable staff time to perform video analysis or investigate sensor alerts.

- Deficiencies in the contract management and processes used to install ISIS equipment have resulted in more than $37 million in DHS funds remaining in General Services Administration (GSA) accounts; delays in installing, testing, and bringing on-line RVS sites that are operational; and 168 incomplete RVS camera sites.

- Efforts to enhance and expand remote surveillance coverage will continue to face numerous challenges, i.e., streamlining the RVS camera site selection process and addressing environmental, cultural, and historic restrictions.

We are recommending that CBP (1) maximize integration opportunities and ensure that future remote surveillance technology investments and upgrades can be integrated; (2) standardize the process for collecting, cataloging, processing, and reporting intrusion and response data; (3) develop and apply performance measures to evaluate whether current and future technology solutions are providing force-multiplication benefits and increasing response effectiveness; (4) continue to work with GSA to resolve contract related claims, financially reconcile funding provided to GSA, and obtain the return of the unused funds to DHS; (5) develop strategies to streamline the site selection, site validation, and environmental assessment process to minimize delays of installing surveillance technology infrastructure; (6) expand the shared use of existing private and governmental structures to install remote surveillance technology infrastructure where possible; and (7) continue to identify and deploy the use of non-permanent or mobile surveillance platforms.

Background

The September 11, 2001, terrorist attacks on the World Trade Center and Pentagon highlighted the urgent need to reevaluate border security risks as well as the resources needed to secure the nation's borders. With the establishment of DHS, the functions and jurisdiction of several border and

security agencies were merged into the Border and Transportation Security Directorate (BTS), which was tasked with securing the nation's borders and safeguarding its transportation infrastructure.[2] Within this directorate, CBP, through its uniformed enforcement services, is responsible for detecting and preventing illegal aliens, terrorists, and contraband from entering into the United States.

CBP officers are responsible for border security at POEs; OBP agents are responsible for border security and control between POEs. OBP, the only federal law enforcement agency policing the nation's land borders, performs this mission by conducting regular land, air, and marine patrols. OBP's statutory authority is outlined in Title 8, United States Code, Section 1357. OBP's strategic plan emphasizes that its top priority is to:

> Strengthen U.S. Borders to prevent entry into the United States of terrorist and terrorist weapons, smugglers and illegal aliens, narcotics, and contraband.

Since joining DHS, OBP's organizational structure and day-to-day operational practices have undergone change.[3] Under the legacy INS, OBP operations were decentralized to three INS regional offices that had operational and administrative oversight over 21 border patrol sectors.[4] As part of DHS, the regional office structure was removed and OBP sector chiefs now report directly to OBP headquarters. OBP has a workforce of more than 12,700 employees, of whom 10,742 are OBP agents assigned to patrol the vast expanse of America's land borders.

The Integrated Surveillance Intelligence System

In the early 1970s, OBP started using technology to assist its agents in remotely detecting illegal aliens entering the United States along its 4,000 miles of border with Canada and 2,000 miles of border with Mexico.[5] OBP began using seismic and magnetic sensors to provide rudimentary warnings of possible intrusions. While the sensors improved detection capability, they resulted in numerous false alarms.

[2] Public Law 107-296, the *Homeland Security Act of 2002*.
[3] Effective March 1, 2003, the functions of INS, of which OBP was a part, were transferred to DHS from the Department of Justice, and INS was abolished.
[4] Recently, OBP eliminated the Livermore Sector and divided the land area among nearby sectors. Within the remaining border sectors are 142 border patrol stations.
[5] The 6,000 miles of border does not include the 1,500 miles of border between Alaska and Canada.

In the early 1980s, an electronic system was introduced to record sensor alerts. Additionally, low-level light television cameras were installed at several known high-traffic locations. In 1988, the ICAD system was introduced and used by OBP to register sensor activity, track agent response, and record results.

In 1998, INS formally established the ISIS program. ISIS equipment was intended to provide continuous monitoring of the borders in all weather conditions. When fully deployed, ISIS was to establish a fully integrated network combining sensor detections with camera video identification capability.

ISIS Equipment

- **Sensors**, primarily seismic and magnetic, buried in the ground, provide remote detection capability. When a sensor detects activity, alerts are sent via radio transmission to an OBP sector or station communications center. This alert is registered in ICAD and displayed on workstation terminals monitored by Law Enforcement Communication Assistants (LECAs). According to OBP, there are more than 11,000 sensors along the northern and southwest borders.

- **RVS systems** provide the primary remote identification capability. RVS components include cameras, mounting poles, radio, and equipment, such as cabling and equipment enclosures. The RVS system includes both color (day) and thermal-infrared (night) cameras, which are mounted on sixty or eighty-foot poles or other structures. RVS camera signals are transmitted to the OBP sector or station communications center via a wireless system such as microwave signal, or, in one sector, via fiber optic cable. Personnel at designated communications centers can control most RVS cameras remotely using toggling keyboards. There are 255 operational RVS camera sites along the northern and southwest borders.

- The **ICAD system** provides OBP with a resource tracking and response coordination capability. ICAD is integrated with sensors so that when a sensor is triggered, an alert is registered in ICAD. The alert creates an event record, or ticket, that is used to record data pertaining to the alert and eventually the result of an OBP agent's investigation. ICAD aids LECAs in tracking OBP agent activities and provides OBP with a means to generate activity reports.

Procurement

Over the life of the ISIS program, different regulations, contracts, and agreements for various durations governed the installation of the RVS sites.[6] According to OBP, there were two primary contract vehicles for RVS installations.[7] Both were GSA federal supply service contracts. In September 1998, INS entered into an interagency agreement with GSA through a Memorandum of Understanding (MOU).[8] According to the MOU, GSA would provide information processing services through task orders to private sector contractors, and GSA would provide the contracting officer and the contracting officer's technical representative. In March 1999, the International Microwave Corporation (IMC) was awarded a contract to engineer, install, manage, and provide remote surveillance equipment and support to multiple sites throughout the United States.

Blanket Purchase Agreement for Remote Video Surveillance Installations

Following the initial award to IMC, OBP requested that a Blanket Purchase Agreement (BPA) be issued to IMC by GSA. OBP cited cost savings as the greatest benefit of a BPA. Specifically, OBP highlighted a unique teaming alliance IMC had with five technology companies, which would result in favorable equipment discounts up to 16 percent below the GSA federal schedule price list. Additionally, OBP stated that IMC had emerged as the principal systems integrator, and that approval of the BPA would help standardize the RVS equipment by eliminating the continual requests from the field for customization. In November 2000, GSA issued a BPA with IMC to support all RVS requirements through September 30, 2004.[9]

Under the terms of the BPA, the contractor was obligated to (1) perform technical and construction feasibility assessments of sites identified by OBP; (2) perform preliminary real estate coordination, which included determining land ownership and property rights; (3) coordinate environmental assessment activities; (4) assist in obtaining permits, zoning approvals, and lease or memorandums of understanding between the government and the land owner; (5) develop preliminary designs, including

[6] This included Federal Acquisition Regulations, GSA federal supply schedule contracts with various vendors, particularly the federal supply schedule contracts with IMC; the MOU between GSA and INS; and, a Blanket Purchase Agreement (BPA).
[7] According to OBP and GSA records, it appears that one primary contract was GS-35F-1103D, through which, (according to OBP) at least $27.8 million was awarded, and the other primary contract was GS-35F-0425J, which was referenced in the BPA. GSA records indicate that there was a third contract for RVS installations: GS05T01BMM2002.
[8] GSA MOU 152053601
[9] BPA GS05KR01BMC0001 was signed during November 2000 for an estimated $200 million in purchases. Only ISIS technology and OBP agent support equipment and services could be ordered under this BPA.

geotechnical surveys, foundation design, and boundary design; (6) deliver, install, and test each RVS component; and, (7) provide system operation and maintenance support, system documentation such as final design plans, and any other documentation or equipment deemed necessary under the approved technical directives (TD).[10]

The BPA included 22 defined contract line item numbers (CLIN), each with a detailed description and corresponding firm fixed price per unit. The CLIN definitions called for "full turnkey" installations of various camera site configurations and support equipment. This standardized the ordering process under the BPA and allowed for the cost of each TD to be calculated by multiplying the quantity of CLINs by the firm fixed price. In addition to the CLINs, the BPA allowed for "other direct costs." Other direct costs were defined as equipment, materials, and services, which fell outside the CLINs but were necessary to complete the installation. These other direct costs were capped at 10 percent of each TD awarded under the BPA.

The BPA could be renewed provided that the federal supply service contract between the contractor and GSA was renewed. That contract was not renewed, and the BPA expired on September 30, 2004. According to OBP, as of August 2005, 255 RVS camera sites and 27 non-camera sites, such as repeater towers, are operational, and 168 RVS camera sites and 38 non-camera sites are incomplete. Of those 255 completed sites, 105 were installed pursuant to TDs issued prior to the BPA.

ICAD Contracting

OBP obtained contract services through GSA for ICAD equipment installation and technical support. In January 2001, a time and materials task order was awarded to HAZMED, Inc. to support all ICAD requirements through September 2001. A new one-year, with four option years, contract was awarded in September 2001. OBP is currently exercising the option year provisions of this contract, which could extend until September 2006.

Sensor Contracting

OBP procured sensors and sensor parts via the DHS Special Purchase Processing Equipment III fixed price contract. Due to new requirements to use narrow (radio) bandwidth sensor equipment, OBP made arrangements to purchase sensors meeting these requirements through an existing DHS

[10] Based on several documents, "TD" was used interchangeably as an abbreviation for Task Directives, Technical Directives, and Task Descriptions. Under the BPA, TDs defined the number and type of RVS sites to be installed and the period of performance for the work to be completed.

Bureau of Immigration and Customs Enforcement contract.[11] Sensors are used until they are not repairable, at which time they are taken out of service and replaced if others are available. These sensors cost approximately $3,500 each.

Capabilities, Limitations, and Requirements

ISIS provides OBP with a remote detection and identification capability. However, there are factors that limit the effectiveness of this technology. For example, (1) sensors are not able to differentiate between illegal activity and legitimate events; (2) RVS cameras cannot automatically detect any activity or movement and are limited by weather; (3) sensors are limited by battery power and RVS cameras have infrastructure requirements that have caused significant installation delays and cost overruns; and, (4) the success of ISIS is ultimately dependent upon the limited availability and capability of staff resources.

Sensors

Sensors are part of the first line of a layered border security strategy. Sensor technology is the most used as well as the easiest and least expensive to install and maintain. The sensor sensitivity level can be adjusted to help filter false alerts. When activity or movement near a sensor meets sensitivity parameters, a radio signal is transmitted and the alert is registered in the ICAD system. When sensors are placed in a pattern, or "sensor string," experienced OBP personnel can estimate the direction and rate of travel and the possible number of intruders based on the sequencing of the alerts, the time lapse between alerts, and the number of alerts transmitted.

Although effective in detecting activity or movement, sensors cannot differentiate between illegal activity and legitimate events. Consequently, nearly all sensor activations must be investigated. The general exceptions are when certain events occur such as earthquakes, area blasting, or severe weather, which could reasonably explain why multiple sensors within a certain area are triggered at approximately the same time.

Moisture, insects, and intentional or accidental physical damage can affect the operation of a sensor. Sensors are susceptible to physical damage from vehicles, machinery, or vandals. Insects penetrating sensors and shorting-out components or corrosion caused by moisture can cause sensors not to function properly. To mitigate the effects of insects, OBP agents apply various chemicals or repellents on or around the sensors.

[11] According to a senior OBP official, Monotron is the only supplier of sensor equipment that can transmit signals using OBP's existing communications equipment.

Limited power supply from batteries can also affect sensor operation. Sensor battery life is based on two primary factors: weather conditions and the number of times the sensor is activated. Sensors do not have battery life indicators but are programmed to send test signals on a periodic basis. When these test signals are not transmitted, this normally indicates that the sensor battery needs to be replaced. OBP personnel routinely replace batteries about every six months. Recognizing that it can be difficult to locate and dig up sensors during certain weather conditions such as snow, it is common practice for northern border sectors to replace batteries during the fall and spring, preferring to replace a battery before it actually needs to be replaced so that the sensor is not out-of-service for an extended period of time during the winter.

Remote Video Surveillance Cameras

Other than having an OBP agent on site, thermal-infrared, low-level light and multiple color cameras provide the most effective means of identification. Since cameras provide a visual means to evaluate activity on a real-time basis, they are the most effective technology used by OBP to differentiate between illegal activity and legitimate events. Cameras with remotely controlled pan and tilt capability can cover a wider field of view than cameras with fixed viewpoints.

However, RVS cameras are limited. RVS cameras do not have the ability to detect movement. Therefore, illegal activity may go unnoticed unless OBP personnel happen to be monitoring video terminals at the time an illegal crossing is in progress. RVS cameras are only operational when electrical power is available. Recognizing the vulnerability to local power outages, one sector we visited installed back-up power to cameras located near corridors with a high volume of illegal alien traffic. Not all camera sites have back-up power sources. Also, extreme weather conditions can affect camera operation. For example, excessively high or low temperatures can cause cameras not to respond to remote pan and tilt commands. On the northern border, OBP sector personnel suggested that all cameras be equipped with heaters to melt snow and ice build-up that otherwise might impede the camera's operation. Likewise, cooled cameras in hot and humid conditions can improve quality resolution.

Infrastructure Requirements

Both RVS cameras and sensors must transmit signals to receivers at OBP sector or station headquarters. RVS camera signals usually are sent via microwave radio communications, and, in one sector, via fiber optic cable. In addition, cameras require that zoom, pan, and tilt commands be sent via radio signals from OBP sector or station headquarters. This generally does

not pose a significant problem if line of sight can be maintained between transmitter and receiver, or unless the signal has to travel a significant distance. However, the terrain along remote areas of the northern and southwest borders is so diverse that few areas are conducive to transmitting radio signals without the use of repeaters, which usually requires the additional construction of repeater towers to relay camera or sensor signals.

In most cases, the installation of both RVS camera sites and repeater towers requires access to land. Assuming OBP is able to negotiate lease agreements or memorandums of understanding with property owners, these areas need to be supplied with electrical power as well. When access to strategically or tactically desirable land cannot be acquired, or is not technically feasible, alternate locations must be used. In some instances, OBP has placed RVS cameras on existing infrastructure belonging to local governments or private utility companies.

For each location where infrastructure is needed, environmental assessments must be performed according to the *National Environmental Policy Act* (NEPA) to determine whether project activities will adversely affect environmental quality.[12] Historically, OBP has funded the U.S. Army Corps of Engineers (USACE) to perform these environmental assessments after the contractor has negotiated property access but before beginning the actual tower and equipment installations.

Due to the time needed to address these non-construction related requirements, RVS camera site installations have taken, on average, 20 months to complete.

Personnel Requirements

The success of ISIS is ultimately based on the availability and capability of three types of personnel: the LECA, the OBP agent, and the CBP-Office of Information Technology (OIT) specialist.

- **LECAs** are primarily responsible for providing radio and dispatch support to OBP agents in the field. They are the coordination point between ISIS and the OBP agent. The LECAs are tasked with monitoring both RVS camera and ICAD terminals. Once they observe suspicious activity or receive a sensor alert notification from ICAD, they radio the information to OBP agents who, in turn, investigate and report their findings. When the results of the OBP agent's investigation are received, the LECA closes the ICAD ticket.

[12] 42 U.S.C. Section 4321, et seq. NEPA requires that all federal agencies analyze the potential effects of proposed federal actions, which significantly affect the environmental quality, including a detailed analysis of alternatives to the proposed actions.

- **OBP agents** respond to the alerts dispatched by the LECAs, investigate the cause of alerts and report their findings. OBP agents also install and maintain sensors. In some sectors, OBP agents are assigned to OBP sector or station communications centers to monitor RVS cameras, especially in areas with a high volume of illegal alien traffic. Where remote surveillance coverage has not been installed, OBP agents conduct air, ground, and marine patrols.

- **CBP-OIT specialists** perform first-level, on-site repairs to RVS cameras.[13] When an RVS camera's zoom, pan, and tilt motor or other electrical components fail, CBP's OIT personnel attempt to repair the equipment on-site. However, cameras that cannot be repaired on-site are sent to the OBP Operations and Maintenance facility in Albuquerque, New Mexico.[14] Also, OIT specialists perform more extensive repairs to sensors, such as replacing electrical components.

Integration

Since its introduction, the ISIS program has had varying expectations. However, it is clear that sensors and RVS cameras were intended to work in conjunction with one another, leveraging the detection capabilities of sensors with the visual identification capabilities of RVS cameras. On February 25, 1999, the INS Commissioner testified before the House Judiciary Committee Subcommittee on Immigration and Claims regarding ISIS and *automated* integration of the RVS cameras and sensors.

> [W]hen a ground sensor is triggered, a signal is sent, the designated camera receives the signal, and the camera then trains on the triggered ground sensor. At the centrally-located video monitoring site, the person monitoring the video screens is alerted to which sensor/camera system has been triggered, and can immediately view the site.

On June 17, 2004, the Under Secretary for BTS testified before the Senate Committee on Commerce, Science and Transportation regarding the *manual* integration of the RVS cameras and sensors.

> When a sensor is tripped, an alarm is sent to a central control room. Personnel monitoring control room screens use the

[13] CBP OIT personnel referred to here were formerly OBP electronic technicians. In October 2004, these positions were transferred to CBP.
[14] Operations and Maintenance facility was established to receive, distribute, and maintain RVS equipment.

ICAD system to manually position RVS cameras in the direction from which the sensor alarm is tripped.

Therefore, whether by automated integration allowing RVS cameras to train on the location of the triggered sensor, or through manual integration, sensors and RVS cameras were envisioned to work together.

Sensors are automatically integrated with the ICAD system, as a sensor alert automatically creates a ticket in ICAD. However, neither sensors nor ICAD are automatically integrated with RVS cameras. OBP tested hardware and software design modifications internal and external to ICAD that would have automated the integration between sensors and RVS cameras. These modifications were "successfully demonstrated," but never deployed because solutions did not meet functional requirements.[15]

For the most part, ISIS information is only available to OBP personnel in a designated sector or station. Although the ICAD system is networked, OBP managers decided to limit sharing of ICAD data between OBP sectors. However, when shared access to ICAD data is authorized, it generally allows adjacent OBP sectors or stations that share a common boundary to exchange information. This facilitates coverage and analysis of illegal alien activity along the seam between sectors or stations. Within an OBP sector, it is possible to access ICAD data from multiple stations. But, sharing RVS camera video images is more constricted. RVS camera feeds terminate at OBP sector or station communications centers similar to a closed circuit television configuration.[16]

Without automated integration between sensors and RVS cameras, LECAs must manually point cameras to areas where sensors have been triggered. The manual integration of sensors and RVS cameras is only possible where sensors and RVS cameras are installed in close proximity. Also, LECAs are required to manually integrate ISIS components by notifying OBP agents of sensor activations or questionable activity detected while monitoring camera video. The Under Secretary for BTS testified on June 17, 2004, that in the future, he expected ISIS to integrate data from Unmanned Aerial Vehicles (UAV), which are discussed later in this report.

[15] According to OBP, during test demonstrations, the signal back and forth between the sensors and the cameras was successful. However, the camera did not consistently train on the location of the triggered sensor. Additionally, the integration solution was unable to deal with multiple sensors near the same camera location being triggered in rapid succession.

[16] Closed circuit television or video differs from broadcast television in that all components are directly linked via cables or other direct means. Therefore, video images may be viewed or recorded only at the termination point.

Force-multiplication

OBP has not developed performance measures to evaluate the effectiveness of ISIS. OBP officials said, however, that such measures were in the process of being developed, as are ways to measure force-multiplication and deterrence.

Nevertheless, OBP officials assert that ISIS has been successful in serving as a force-multiplier in that it frees the use of the limited number of OBP agents who would otherwise be needed to monitor the border.

Transition to the America's Shield Initiative

Recognizing the need to improve border surveillance and remote assessment and monitoring technology, OBP began developing ASI in June 2003, as a program to integrate surveillance technology, communications, and visualization tools. OBP's goal is to deliver new operational capability incrementally over a six-year acquisition period, while maintaining and modernizing ISIS. Current ISIS system components represent a very small part of the overall capability envisioned under ASI.

Modernization measures of ISIS equipment under ASI may include additional surveillance structures, upgraded and expanded surveillance equipment, and significantly enhanced detection and monitoring capabilities. The measures may also include improved links to OBP agents to provide direct visual or other detection data as well as integrating new surveillance technologies including air, ground, and marine. Underlining any surveillance enhancements will be the need to provide all-weather, 24-hour capability.

According to OBP, expanded use of surveillance technologies would be an effective force-multiplier, enabling agents to reduce requirements for static observation and provide an intelligence-based response. ASI will incorporate a means to evaluate the performance and effectiveness of enforcement actions. It is envisioned that ASI will collect performance metrics and provide managers with reports and analyses of its efficiency and effectiveness in enhancing the agents' enforcement capabilities. The chief of the Border Patrol will prioritize ASI deployments based on threat models. For example, the Arizona border, which experiences half of the nation's illegal alien traffic, will likely be an initial deployment priority.

DHS estimated that full implementation of ASI will cost approximately $2.5 billion.[17] Because of the cost, the DHS Deputy Secretary's approval was required to initiate work. That approval was granted in September 2004.

CBP officials advised that they plan to establish ASI requirements and objectives and then hire a contractor to serve as a prime integrator. The contractor will be responsible for designing and building an integrated system that best meets OBP objectives. Since receiving approval to proceed with ASI, OBP has been working with CBP-OIT and a consulting contractor to identify and refine ASI requirements. OBP expects to select the prime integrator by July 2006.

Concurrently, OBP has been working with the Science and Technology Directorate (S&T) to identify potential technology solutions to address impending ASI requirements.[18] OBP field personnel participate in operator workshops organized by S&T's Office of Programs, Plans and Budget (PPB).[19] These workshops focus on capability requirements, not specific technologies, and seek to identify the most urgent needs of DHS programs. OBP will continue to use this forum to identify capability gaps to promote research, development, testing, evaluating, and fielding technology solutions.

Once ASI is further refined and the prime integration contractor identifies specific technology requirements to meet OBP's objectives, S&T anticipates that the work they have completed to date can be quickly integrated into ASI. As other ASI requirements become apparent, S&T will address those requirements for future ASI integration.

Unmanned Aerial Vehicles for Border Security

Another technology advancement OBP is pursuing is the use of UAVs. OBP began using UAVs in support of the Arizona Border Control Initiative in June 2004, after nearly a year of planning, coordinating, and evaluating the concept by S&T and BTS. S&T examined the technical capabilities of the UAV platform, while OBP developed tactical uses for the UAVs. OBP flew an Israeli-made Hermes UAV during June through September 2004.

In FY 2005, Congress provided $10 million for the continued use of UAVs along the southwest border. In October 2004, a memorandum from the DHS Secretary directed that UAVs become an operational asset along the

[17] In October 2004, the DHS Deputy Secretary estimated that the preliminary cost to fully fund the program would be $2.5 billion.
[18] S&T is the primary research and development organization within DHS.
[19] PPB provides the strategic and technical vision for S&T.

southwest border. In support of the Secretary's directive, S&T made arrangements for Northrop Grumman to provide UAV services using an RQ-5 Hunter UAV platform during the month of January 2005. After January 2005, the flights ended and OBP, with support from S&T, began refining platform and sensor package requirements in preparation for issuing a Request for Information for a UAV system.

On August 30, 2005, CBP announced that it had awarded a $14.1 million contract to General Atomics Aeronautical Services, Inc., to deliver, operate, and maintain one Predator B UAV platform and sensor package. This is a one-year contract, with the option to extend the contract thereafter. According to OBP, the Predator B is more capable than the UAVs used during test flights, as well as more expensive to operate. The onboard electro-optical sensors will aid OBP agents in apprehending illegal aliens, confirming the cause of sensor alerts, and surveying remote areas of the border.

Operations

During testing, the Hermes and Hunter UAVs were primarily used to support apprehension of illegal aliens who had already been spotted by other means. After illegal aliens were identified, the UAV was flown to the vicinity of the contact. Once the UAV operators acquired visual contact of the illegal aliens by manually searching with the craft's onboard cameras, the UAV was used to monitor the movement of the illegal aliens as well as to guide OBP agents to them. One OBP official credited a UAV-assisted apprehension for the capture of 81 illegal aliens by only four OBP agents. Had the UAV not been in place to monitor the location and movement of the illegal aliens when they break up into smaller groups and head in multiple directions, the OBP official estimated that only 16 would have been apprehended.

All test flights to date have been along the southwest border. Although the Under Secretary for BTS testified on June 17, 2004, that he expects ISIS to integrate data from UAVs, currently both systems are operated independently.

Coordination

While DHS has approved UAVs for operational use, Federal Aviation Administration (FAA) flight restrictions limit the use of UAVs in the National Airspace System (NAS) because they do not possess an acceptable "detect, sense and avoid" capability.[20] According to an FAA official, an

[20] According to one FAA official, "detect, sense and avoid" is the ability to of an aircraft to detect other aircraft, terrain or other civil airspace users in its flight path and maneuver in order to avoid a collision. This is contrasted with the

acceptable solution to this limitation is still ten years away. FAA does not consider onboard cameras, positioned to observe targets on the ground, to be adequate for meeting "detect, sense and avoid" requirements. However, due to the dramatic increase in the use of UAVs in both the public and private sectors in recent years, on September 16, 2005, the FAA Flight Technologies and Procedures Division issued a policy memorandum to be used in determining whether UAVs will be allowed to fly in the NAS.

According to FAA's policy memorandum, UAV pilots must have an understanding of Federal Aviation Regulations applicable to the airspace where the UAV will operate. Currently there are no federal licensing requirements to operate UAVs. However, according to one FAA official, in the near future UAV pilots will most likely be required to be certificated pilots of manned aircraft. Currently, OBP is not training any of their agents to operate UAVs.

The FAA supports UAV flight operations that can demonstrate an acceptable level of safety. For these purposes, the FAA policy memorandum outlines a process by which UAV operators might be able to demonstrate an acceptable level of safety by performing what FAA calls a system safety study. A system safety study might include a hazard analysis, risk assessment, and other appropriate documentation that concludes that a collision with another aircraft, parachutist, or other civil airspace user is highly unlikely. Additionally, if UAVs are going to fly over congested areas, heavily-trafficked roads, or an open-air assembly of persons, the operator must provide information that establishes that the risk of injury to persons on the ground is highly unlikely. According to FAA, OBP is documenting air and ground traffic information along the southwest border for the purpose of including this information as part of their system safety study. FAA's policy memorandum also includes a provision that allows UAVs to be used for matters of national security when, under normal circumstances, it does not conform to FAA policies. When operating UAVs under these circumstances, FAA requires that the operator assume all risks.

Limitations

While the UAVs that were tested are able to stay airborne for up to 20 hours, which surpasses any current capability of aircraft in OBP's fleet, there are significant limitations to the UAV system. Weather conditions can impact the operational capabilities of UAVs. Dense cloud cover limits the visual acuity of some sensor and camera packages. Also, icing conditions and thunderstorms cause difficulty for UAV flights.

traditional "see and avoid" function, which involves the human eye of a pilot looking out the window of the aircraft to "see and avoid" potential obstacles.

UAVs remain very costly to operate and require a significant amount of logistical support as well as specialized operator and maintenance training. Operating one UAV requires a crew of up to 20 support personnel. OBP officials mentioned that the cost to operate a UAV is more than double the cost of manned aircraft, and that the use of UAVs has resulted in fewer seizures. However, the fact remains that UAVs can stay on station for an extended period of time, which is a distinct advantage over manned air support. According to OBP, the Hermes UAV costs $1,351 per flight hour and the Hunter costs $923. Those figures included acquisition costs, operations and maintenance costs, and the salaries and benefits of the pilots, payload operators, and mechanics. Flight hour costs were based on leasing the tested UAVs as opposed to a purchase, which OBP says would be less expensive.

Results of Review

ISIS Has Not Been Integrated

Despite a federal investment of more than $429 million since 1997, ISIS components have not been integrated to the level predicted at the program's onset. RVS cameras and sensors are not linked in any automated fashion. At each sector we visited, sensor alerts did not automatically activate a corresponding RVS camera to pan and tilt in the direction of the triggered sensor. At most sectors we visited, cameras had to be manually operated via toggling control keyboards. In one sector we visited, camera positions and views were fixed.[21]

To date, only limited automated integration has taken place. For example, ICAD and sensors are integrated and ICAD is networked and can be shared with other sectors. According to one senior OBP official, OBP is planning to allow sectors to view "read-only" ICAD data via the ICAD intranet website.

RVS camera surveillance video can be viewed only at one designated OBP sector or station communications center.[22] According to OBP officials,

[21] The six cameras the sector currently uses do not have a pan and tilt feature. These cameras were not deployed as part of ISIS. Of the six cameras, two belong to Customs and Border Protection, and one belongs to the Canadian Railroad for which the sector has received permission to receive feeds.

[22] When RVS camera systems were designed, each TD called for the installation of a number of camera sites along the border and one control room where the camera video is sent and can be viewed. The control rooms are installed in either a station or sector communications center. The communications infrastructure for an RVS camera can only send the video signal to a single control room regardless of whether that control room is in a station or sector communications center.

sharing surveillance video with other locations would require the infrastructure necessary to transmit, receive, and monitor signals from desired camera locations. Even if ISIS was fully integrated, due to a limited number of operational RVS sites (255 nationwide), integration opportunities would be limited to the areas near these sites. The remainder of the border is covered by sensor technology only or not covered by any remote surveillance technology.

ISIS funding has been provided on an annual basis since 1997. However, the amount that would be available to ISIS planners often was not known or available until late in the fiscal year. Therefore, the ability to plan and schedule system enhancements was limited. Neither the RVS or ICAD contracts required the automated integration of RVS cameras with sensors. Also, as one senior OBP official explained, such automated integration technology was not affordable at the time the contracts were issued.

The lack of automated integration undercuts the effectiveness and potential of ISIS. Since no automated integration exists between RVS cameras and sensors, the integration of information from these two sources becomes the responsibility of the LECA. The LECA is required to select the appropriate RVS camera, manually maneuver the camera in the direction of the sensor and attempt to identify the cause of the sensor alert. At one location we visited, only one LECA was on duty performing radio-dispatch duties, processing sensor alert information via ICAD, and monitoring 32 cameras.

Additionally, without automated integration, the need for additional equipment to be available to perform manual integration increases. Without the necessary equipment, the effectiveness of ISIS is further lessened. At each sector we visited, there were more RVS cameras than toggling keyboards, allowing only a few cameras to be controlled at one time. Thus, the number of functioning toggling keyboards limits active camera monitoring. The sector we visited with 32 cameras only had three toggling keyboards.

Recommendation 1: We recommend that the Commissioner, Customs and Border Protection, maximize integration opportunities and ensure that future remote surveillance technology investments and upgrades can be integrated.

OBP Could Not Demonstrate Force-Multiplication Advantages or Performance-Measuring Results to Validate the Benefits of Technology Investments

Senior CBP and OBP officials have made repeated statements in congressional testimony and program documents that ISIS is a force-

multiplier. During interviews with OBP officials at headquarters and in the sector offices, we were told that remote surveillance technology was a force-multiplier. However, OBP could not provide any quantifiable data to support this claim.

Furthermore, none of the sector officials reported they were analyzing the accuracy of alerts. Instead, sector intelligence personnel use sensor data to evaluate traffic patterns and to position OBP agents and additional sensors to intercept illegal aliens more effectively.

A senior OBP official at headquarters said that INS never paid much attention to the *Government Performance and Results Act of 1993* standards until 1998 or 1999.[23] Therefore, prior to 1999, few statistical indicators or performance measurement standards were used to analyze ISIS return on investment. Now, six years later, such performance measures are under development. A senior OBP sector official said that he participates in a national planning group that is working on developing a way for OBP to measure both force-multiplication and deterrence.

Several OBP sector personnel said that it was difficult to measure force-multiplication, but that ISIS prevents OBP agents from having to respond to false alarms. Another OBP sector official indicated that ISIS allows OBP agents to respond to legitimate intrusions in a timely manner, but that measuring the degree of effectiveness is difficult.

Reasons varied for not having developed force-multiplication metrics. OBP officials pointed out that to measure accurately force-multiplication benefits of ISIS technology, two types of information are required: the number of attempted illegal entries and the number of attempts that were successful. With this information, OBP could perform trend analysis as ISIS equipment is introduced or increased in an area to determine if ISIS is aiding in the apprehension of those who illegally crossed the border or deterring attempted illegal entries. Since this information is not easily obtainable, OBP must consider other indicators to measure force-multiplication and response effectiveness.

ICAD Data is Incomplete and Unreliable for Measuring Force-Multiplication

OBP officials acknowledged that ICAD data could be used to analyze force-multiplication and response effectiveness. However, because of the numerous variables involved in cataloging information in ICAD, they also acknowledge that ICAD data would be of limited value and stated that

[23] The *Government Performance and Results Act of 1993* holds federal agencies accountable for achieving program results.

conclusions drawn from this data would vary significantly at times. Several data entry steps are necessary for ICAD data to be useful in determining force-multiplication benefits and response effectiveness. If any of these steps were not completed, the ICAD data would be incomplete.

One senior OBP official described the ICAD data collection process as follows:

1. Sensor alerts automatically create a ticket in ICAD. If questionable activity is detected while monitoring RVS camera video or a citizen or another agency reports illegal alien activity, the LECA manually creates a ticket in ICAD.

2. Once an ICAD ticket is created, the LECA must radio the intrusion alert to an OBP agent in the field.

3. The OBP agent must acknowledge and then investigate the alert.

4. After investigating the alert, the OBP agent must report his or her findings to the LECA.

5. Once the LECA receives this information, the LECA must enter the information into ICAD.

LECAs may not always have time to advise an OBP agent of sensor alerts or camera observations due to the need to address higher priority events such as vehicle stops, patrol apprehensions in progress, or anytime officer safety is an issue. During this time, LECAs may be restricted from using the radio until such time as the higher priority events stabilize and routine communications can resume. Similarly, OBP agents may not be available to respond in a timely manner due to limited staff or because they are responding to an earlier or higher priority call. If there is a significant delay between the time the possible intrusion occurred and the time the OBP agent is available to investigate, the ticket may simply be cleared as "Unidentified," "Not Available," or "Unknown."[24] Based on these variables, OBP officials are hesitant to use ICAD data to accurately and consistently measure force-multiplication or response effectiveness.

Furthermore, ICAD data is not recorded consistently. According to our analysis of the 13 ICAD response categories used by the six sectors in our

[24] According to OBP, "Unidentified" means that an investigation into the incident may have been performed, but no OBP agent reported its result to the communications center; "Not Available" means that an investigation into the incident was performed, and an OBP agent currently has no result for the incident, though a result may be forthcoming after further investigation; and, "Unknown" means that an investigation into the incident was performed, and an OBP agent cannot determine what caused the incident.

sample, there was not a common category that was used by all six sectors.[25] Also, it appears that different OBP sectors used ICAD result categories differently. For example, one southwest border sector in our sample labeled 10,252 ICAD sensor tickets as "Unidentified" and only three tickets as "Not Available," while another southwest border sector in our sample labeled 7,503 ICAD sensor tickets as "Not Available" and none as "Unidentified."

Moreover, some OBP sectors are recording certain events in ICAD while other sectors are not. For example, one southwest border sector in our sample recorded 244 vehicle stops in ICAD, while another southwest border sector in our sample did not record any vehicle stops. While it is possible that some sectors might not encounter certain types of activities, it is unlikely that that explains this situation given the general definition of these categories.

Using sample ICAD data, we determined the percentage of apprehensions attributed to sensor alerts and other detections recorded in ICAD. However, OBP officials cautioned against using the number of apprehensions to measure effectiveness because of external factors that directly affect the number of apprehensions. These factors include the number of OBP agents available to respond to sensor alerts or video observations, intercept distances, and the volume of illegal traffic at any given time. Accordingly, the more OBP agents that are available to respond to intrusion alerts combined with a lower rate of illegal traffic, the greater the probability of apprehensions. Conversely, when the rate of illegal traffic is high and the number of OBP agents available to respond is low, the lower the probability of apprehensions.

OBP officials believe that RVS cameras serve as a deterrent to illegal border crossings. An OBP official said that once illegal aliens learn where RVS cameras sites are located, they may choose not to cross at those locations. Several OBP officials said that an effective deterrent would actually result in a decreased number of apprehensions. As one senior OBP agent asked rhetorically, "Is it better to deter illegal entry or arrest the same number after they have crossed the border?"

Despite the reasons given for not having a means by which to measure force-multiplication and response effectiveness, ICAD data is the only data source currently available by which to evaluate force-multiplication and response effectiveness. Without any measurable indicators, there is no quantifiable assurance that remote surveillance technology has increased

[25] Response categories included "Acknowledged, No Unit Available, No Response, On Site, Agency, Enroute, No Need, Delay, Not Acknowledged, Response, Other Agency Responding, Busy and Off Duty." Result categories included "Apprehension, Animal, Got Away, Legitimate Traffic, Agent, Falsing, Local Traffic, Not Available, Turn, Unidentified, Weather, No Violation, Train, Multiple Violations, Outbound, Repair, Equipment, and Unknown."

OBP's capability to monitor the U.S. borders and to detect and respond to illegal intrusions.

Recommendation 2: We recommend that the Commissioner, Customs and Border Protection, standardize the process for collecting, cataloging, processing, and reporting ICAD intrusion and response data.

It is Questionable Whether ISIS has Increased Effectiveness

Even if ICAD data were consistently and fully cataloged, we question whether remote surveillance technology is providing force-multiplication benefits or increasing response effectiveness. According to our analysis of sample ICAD data, non-ISIS sources of illegal alien detection proved to be as effective based on a percentage of apprehensions per ICAD ticket as RVS camera detections.[26] Non-ISIS detections are primarily observations by citizens, OBP agents, or other agency personnel. Along the northern border, non-ISIS sources were more effective than RVS camera detections, and both non-ISIS sources and RVS cameras performed better than sensors based on a percentage of arrests per ICAD ticket.[27]

Our analysis of sample ICAD data also indicated that more than 90 percent of the responses to sensor alerts resulted in "false alarms," meaning that OBP agents spent many hours investigating legitimate activities.

Finally, our analysis of sample ICAD data suggests that additional OBP personnel are needed to integrate and respond to remote surveillance and detections, based on current ISIS capabilities.

[26] The sample included all tickets entered into the ICAD system during five 24-hour periods during April and May 2005. Most ICAD tickets are generated because of a sensor alert. In both the northern border and southwest border samples, there were 32,741 total ICAD tickets, of which 31,787 were generated because of a sensor alert. The rest, 954, were generated because of a camera detection, vehicle stop, officer observation, other agency observation, citizen observation, air observation, or some other source.

[27] Although RVS camera detections and non-ISIS detections resulted in a higher percentage of apprehensions, this percentage can be misleading if compared to sensor detections. ICAD tickets resulting from RVS camera observations are manually entered into ICAD after LECAs viewed questionable activity, whereas sensor alerts are automatically sent when sensor sensitivity parameters are met. As a result, fewer ICAD tickets stemming from RVS camera detections will be entered into ICAD, resulting in a higher percentage of apprehensions per ICAD ticket. ICAD data we sampled did not indicate when sensors and cameras were used in conjunction with one another.

Table 1 - Southwest Border ICAD Ticket Results

Ticket Source	Number of ICAD Tickets	Apprehensions		Staging, Turn or Got Away	Identified False Alarm	Unidentified, Unknown or Not Available
Sensor Alerts	29,710	252	< 1 %	3 %	34 %	62 %
RVS Camera Observations	155	89	57 %	41 %	1 %	0 %
Non-ISIS Sources	780	382	49 %	4 %	40 %	7 %

Source: OIG analysis of OBP ICAD report data. Note: Rows may not equal 100 percent due to rounding.

For the three southwest border sample sectors, 57 percent of RVS camera detections, 49 percent of non-ISIS detections, and less than one percent of sensor detections resulted in apprehensions.

Because of the small percentage of apprehensions attributed to sensors, we performed a closer examination of the 29,710 ICAD tickets generated by this source. We learned that LECAs and OBP agents were unable to determine the cause of 62 percent of the sensor alerts because the LECA was unable to communicate the alert to the agents in a timely manner, no agent was available to respond to the dispatch, or it took the agent too long to get to the sensor location. Those sensor alerts were cleared in ICAD as "Unidentified," "Not Available," or "Unknown." Some of these alerts could have represented illegal aliens that crossed the border and were not apprehended, albeit a small percentage based on the analysis of the remaining 38 percent of sensor ICAD tickets for which the cause was determined.

The cause of 62 percent of ICAD tickets in the sample was not determined. This suggests that staffing resources were not adequate to contend with sensor alerts that were activated, on average, every 44 seconds.

According to our analysis of the 38 percent of ICAD tickets for which the cause was determined:

- Ninety percent were caused by something other than illegal alien activity, such as local traffic, outbound traffic, a train, or animals. An OBP agent investigation was required to determine the cause of these alerts.

- Another two percent were also caused by something other than illegal alien activity. However, an OBP agent investigation was not required to

determine the cause. These sensor alerts were attributed to malfunctioning sensors, repair work, or weather.

- Two percent resulted in apprehensions of illegal aliens.

- Six percent were listed as a "turn,"[28] a "got-away,"[29] or "staging."[30] Each of these indicates instances where sensors detected illegal aliens, but they were not apprehended.

Table 2 - Northern Border ICAD Ticket Results

Ticket Source	Number of ICAD Tickets	Apprehensions		Turn or Got Away	Identified False Alarm	Unidentified, Unknown or Not Available
Sensor Alerts	2,077	5	< 1 %	< 1 %	92 %	7 %
RVS Camera Observations	6	0	0 %	17 %	83 %	0 %
Non-ISIS Sources	13	2	15 %	46 %	38 %	0 %

Source: OIG analysis of OBP ICAD report data. Note: Rows may not equal 100 percent due to rounding.

In the three northern border sectors in our sample, 15 percent of non-ISIS detections and less than one percent of sensor ICAD tickets resulted in apprehensions. No apprehensions were attributed to RVS camera ICAD tickets. However, because OBP officials have identified deterrence as one positive, yet unmeasured benefit of a camera site, this result is not necessarily viewed negatively. Additionally, one sector in the sample did not have RVS camera sites installed.

The ability of OBP personnel to determine what caused a sensor alert in the northern border sample sectors was markedly better than those sectors in the southwest border sample. The northern border sample included 2,077 sensor alert tickets, which is equivalent to a sensor being activated every 10 minutes.

[28] "Turn" means an investigation into the incident yielded no apprehensions because the individual or individuals who entered the United States illegally turned back and exited the country when confronted by agents.
[29] "Got-away" means an investigation into the incident determined that the individual or individuals who entered the United States illegally evaded agents and escaped apprehension.
[30] "Staging" means that an investigation is pending, and OBP agents or camera operators are monitoring individuals who they suspect will cross the border. However, OBP officials stated that "staging" is when illegal aliens cross the border by a few yards and wait for any OBP agent response before proceeding further into the United States. "Staging" was only recorded in one of the three sample southwestern border sectors.

A closer examination of these tickets revealed that LECAs and OBP agents were unable to determine the cause of seven percent of the sensor alerts because the LECA was unable to communicate the alert to the agents in a timely manner, no agent was available to respond to the dispatch, or it took the agent too long to get to the sensor location. Those sensor alerts were cleared in ICAD as "Unidentified," "Not Available," or "Unknown." Some of these alerts could have represented illegal aliens who crossed the border and were not apprehended, albeit a small percentage, based on the analysis of the 93 percent of sensor ICAD tickets for which the cause was determined.

According to our examination of the 93 percent of sensor ICAD tickets for which the cause was determined:

- More than 95 percent were caused by something other than illegal alien activity, such as local traffic, outbound traffic, a train, or animals. An OBP agent investigation was required to determine the cause of these alerts.

- Another five percent were also caused by something other than illegal alien activity. However, an OBP agent investigation was not required to determine the cause. These sensor alerts were attributed to malfunctioning sensors, repair work, or weather.

- Less than one percent resulted in apprehensions of illegal aliens.

- Less than one percent were listed as a "turn" or a "got-away." Both of these indicate instances where sensors detected illegal aliens, but they were not apprehended.

This analysis demonstrated that non-ISIS source detections are an effective means to survey borders based on a percentage of apprehensions per ICAD ticket.[31]

[31] In the future, non-ISIS detections may involve more organized volunteer citizen action groups such as the Minuteman Project, which organized a 30-day vigil along the Arizona border during April 2005. During that time approximately 800 volunteers reportedly shut down a 20-mile stretch along the Arizona border near Naco to illegal aliens by using a simple spot-and-report type of operation. While the exact numbers vary depending on the source, OBP agents credited the civilians with cutting apprehensions in that area from an average of 500 a day to less than 15 a day, with the Mexican government estimating that the number of those attempting to cross the border decreased by half during the patrol period. The CBP Commissioner praised the volunteers' efforts and testified before Congress that trained civilian patrols could be an effective force-multiplier. In July 2005, U.S. Representative John Culberson introduced legislation, H.R. 3622, the *Border Protection Corps Act*, to create a Border Protection Corps, allowing the governors of states along the northern and southern borders to name civilians to work as sworn law enforcement officers for border protection, using $6.8 billion in unused DHS first-responder funds.

According to our analysis of sensor alerts along both U.S. borders, 90 percent or more were false alarms. Therefore, despite claims that ISIS prevents OBP agents from having to respond to false alarms, the analysis indicates that OBP agents are spending many hours investigating legitimate activities primarily because sensors cannot differentiate between illegal activity and legitimate events, and because there are too few operational RVS camera sites available for OBP personnel to evaluate the cause of an intrusion alert remotely.

Finally, based on our analysis, without the necessary personnel to perform video analysis, or investigate sensor alerts, force-multiplication benefits are minimized and illegal aliens may be gaining entry into the United States. Based on OBP data as of March 2005, while the number of OBP agents increased to 10,742 from 9,487, an increase of 1,255 OBP agents since September 11, 2001, the total number of LECA positions actually decreased to 241 from 244 after September 11, 2001. At one location we visited, one LECA was on duty to perform primary radio-dispatching duties, process sensor alerts, and monitor 32 cameras. At another sector, there were only eight LECAs to staff a 24-hour, seven-days-a-week operation. Two sectors we visited assigned OBP agents to communications centers to monitor RVS camera video in high volume illegal alien traffic areas, and one sector we visited used military reserve personnel to perform LECA duties. One senior sector official said he did not need any more OBP agents until he got more LECAs to support them.

In summary, the sample ICAD data suggest that the use of current ISIS remote surveillance technology yields few apprehensions as a percentage of detection, especially when compared to non-ISIS surveillance and detection sources, results in needless investigations of legitimate activity, and is staff intensive.

Recommendation 3: We recommend that the Commissioner, Customs and Border Protection, develop and apply performance measures that can evaluate whether current and future technology solutions are providing force-multiplication results and increasing response effectiveness in monitoring and detecting illegal intrusions along U.S. borders.

OBP's Oversight of Contract Activities Related to RVS Equipment Installations was Ineffective

Weak project management and contract oversight, exacerbated by frequent turnover of ISIS program managers, resulted in RVS camera sites not being

completed, leaving large portions of the border without camera coverage.[32] In addition, completed work was not finished in a timely manner, and millions of dollars in RVS funding remain unused in GSA accounts.

Based on our analysis of OBP and GSA records, 25 TDs were not completed. The total amount awarded for these TDs was $58.4 million. Of that amount, $33.9 million has been paid to the contractor for this partially completed work. According to OBP records, 168 RVS camera sites and 38 non-camera sites have not been completed. As a result, OBP agents must address these coverage deficiencies with manned patrols. Six of these incomplete TDs that should have produced 41 RVS camera sites resulted in just 28 operational RVS camera sites. However, the documents provided did not separate the cost of individually completed sites. Therefore, the total amount awarded and invoiced for these completed RVS camera sites are included in these figures for incomplete TDs.[33]

According to the BPA and the project's Statement of Work, the ISIS project manager was authorized to (1) initiate work by issuing TDs to the contractor, oversee all work performed as a result of the TD, and generally conduct monthly conference calls with the contractor and GSA to oversee contractor performance; and, (2) certify correct and properly supported invoices, thereby accepting services, and return the certifications to the contractor, who would forward the invoice and certification to GSA for payment. Although the contracting officer and the contracting officer's technical representative were GSA employees, it was incumbent upon OBP to oversee contractor performance and certify contractor invoices. Nonetheless, there is only limited evidence that OBP monitored contractor performance or fulfilled its responsibilities under the BPA to certify invoices.

OBP's Oversight of Contractor Performance was Ineffective

To test the adequacy of contracting oversight, we reviewed procurement documents for a sample of seven RVS installation TDs, six issued under the BPA and one issued prior to the BPA.

[32] In a series of audit reports beginning in early 2003, GSA OIG identified inadequate management controls and numerous improper contract activities on the part of GSA's Federal Technology Service, including activities related to RVS installations and contracting. Those audits are included in the "Compendium of Audits of the Federal Technology Service Client Support Centers" dated December 14, 2004. GSA OIG's audits were of GSA's procurement practices and not of the overall efficiency, effectiveness, or management of the RVS program. Conversely, our review was of OBP's use of remote surveillance technology, including RVS equipment, and not an audit of its procurement practices. Nonetheless, while conducting our review, we encountered certain contract management issues that adversely affected the timely installation of RVS equipment.

[33] According to GSA data, the total contract award for these six TDs was $11.7 million. As of August 2005, the total amount paid to the contractor was $6.5 million.

For the six TDs issued under the BPA, periodic monthly performance reviews were conducted and conference calls were held. Documentation provided by OBP did include monthly status reports that had been prepared by the RVS contractor and minutes of conference calls. As evidenced by the incomplete camera sites, the monthly status reports that were completed and the conference calls that were held did not ensure that the RVS contractor finished RVS installations before the BPA expired.

Despite the evidence that OBP conducted some contractor oversight, contractor installations proceeded slowly. According to OBP documents, every TD in the sample included a specified period of performance; however, invariably the periods of performance were extended multiple times. This considerably increased the time required to complete projects. None of the TDs in the sample were completed on or before their original periods of performance. It is unclear who approved the performance extensions. However, there is little evidence that OBP objected or effectively inserted itself in the RVS procurement process to ensure satisfactory contractor performance.

For example, one TD was issued on May 22, 2001, for Phase I installation work at a southwest border sector and on April 8, 2002, for Phases II and III.[34] Each work order had a period of performance of 12 months, which meant the project should have been completed by April 8, 2003. However, the period of performance was extended five times. The last period of performance extension allowed the work to continue until September 30, 2004, the day the BPA expired, for a total extension of slightly less than 18 months. Performance extensions were granted because of environmental assessment work and land lease issues. According to OBP, as of August 2005, 12 RVS camera sites and two non-camera sites remain incomplete for this TD.[35]

In another example, a TD for one northern border sector was issued on May 15, 2001, for Phase I installation work and on March 19, 2002, for Phase II and III installation work. Both of these work orders had 12-month performance periods. These work orders were extended three times, and ultimately all three phases of work were extended through September 30, 2004. Although the performance period for Phase I work was extended for slightly more than 28 months, no poles or cameras were ever installed.

[34] RVS installation work was divided into three main phases. Phase I, administrative preparation, included environmental assessments, rights of entry, real estate issues, permits, power availability, geotechnical surveys, access reports, and surveys. Phase II, ground breaking, included pole installation, utility hook up, and other related construction. Phase III included installation of cameras, transmission lines, consoles, the control room, and other related electronics.

[35] According to OBP records, these 14 sites are in Phases II or III.

According to OBP, as of August 2005, eight RVS camera sites and four non-camera sites remain incomplete for this TD.[36]

OBP Certified Few Contractor Invoices Prior to Payment

According to OBP and GSA records, most contractor invoices were paid without OBP certification. Procedurally, OBP should have certified correct and properly supported invoices, thereby accepting services, and returned the certifications to the contractor, who would forward the invoice and certification to GSA for payment. However, for the six TDs in our sample, GSA paid 58 contractor invoices without documented certification.

Overall, OBP rejected few invoices, and most invoices were not addressed (either accepted or rejected) in OBP invoice certification documents. OBP has hired Performance Management Consulting (PMC) to assist in verifying contractor invoices and closing TDs. As evidence that OBP certified invoices, OBP provided copies of email messages written primarily by PMC employees recommending payment of invoices submitted by the RVS contractor and rejecting a few. For example, for two southwest border TDs in our sample, we reviewed 19 RVS contractor invoices. For those two TDs, only six invoices were recommended for payment in the certification emails. According to GSA records, 39 invoices submitted by the contractor for these two TDs were paid in full. For the other four TDs in our sample that were issued under the BPA, only one invoice was approved in these certification emails, while GSA records indicate 26 invoices for those four sample TDs were paid in full. For our six sample TDs, no invoices were rejected. The certification emails did include rejections of a few invoices for TDs that were not in our sample.

Currently, OBP is certifying invoices after the invoices have been paid. GSA records indicate that almost every invoice submitted was paid in full. With PMC's assistance, OBP is seeking refunds from the contactor for goods and services that were invoiced and paid but not delivered. OBP cited an example where PMC had determined that for one TD, IMC over billed the government by approximately $9,000. As many of the TDs have not been completed and the BPA has expired, OBP must reconcile costs incurred by the contractor on a time and materials basis or based on a percentage of CLIN work that has been completed. For example, one OBP official indicated that the ISIS program management office had certified a 2002 invoice during 2005.

According to GSA, the GSA contracting officer's technical representative was supposed to ensure that OBP received and approved contractor

[36] According to OBP records, these 12 sites are in Phase I.

invoices. GSA agreed that, in practice, there was confusion about the responsibilities of OBP and GSA and, as the project grew and became more complex, the potential for error and pressure to keep on schedule increased. Nonetheless, OBP was obligated to certify invoices, and there is minimal evidence that it fulfilled that obligation. This resulted in payment to the contractor for unverified goods and services.

There is some evidence, however, that OBP attempted to bring the contractor into compliance with the BPA. On September 9, 2003, the ISIS program manager wrote a detailed letter to the contractor outlining a litany of concerns with respect to the contractor's performance. Among other things, the letter cited inefficient financial tracking and cost control, inefficient inventory control, a failure to meet required deadlines and deliverable due dates, and a failure to notify the government of impediments to installations. The letter made several recommendations for remediation.

However, GSA complicated OBP's efforts. In October 2003, GSA concluded that BPA invoices could not be submitted for construction-related expenses. According to the MOU, funds for RVS installations were directed to the GSA "Information Technology (IT) Fund." On October 9, 2003, the GSA contracting officer wrote a letter to IMC instructing the company not to submit any invoices for non-IT related work. This letter also instructed the contractor to disregard OBP's letter of September 9, 2003. According to GSA's letter, the GSA contracting officer is the only authority who can provide contractual direction and OBP's letter was not legally binding. Despite this correspondence, it appears GSA continued to pay invoices that the contractor submitted after this letter was sent.

The MOU was signed in September 1998. It took GSA five years to realize that construction-related expenses were being paid from the IT Fund. The installation of RVS sites involves construction-related activities, particularly installing poles for cameras and related infrastructure, including repeater towers and power supplies. In essence, the letter from the GSA contracting officer was a stop work order. It does not appear that GSA coordinated this action with OBP.

RVS Installation Funds Remain Unspent in GSA Accounts

According to our analysis of OBP records, at least $16 million in OBP funds for RVS camera installations remains unspent in GSA accounts for the TDs we sampled. For the same TDs, GSA records indicate that $5.3 million remains unspent. According to the OBP documentation, $27.2 million in RVS funding was transferred to GSA, which is over $5.9 million more than GSA records show as having been received. Conversely, GSA data indicates $5.1 million more in invoices for these six TDs than what OBP

records showed. As the roles and responsibilities of OBP and GSA were unclear, both entities kept poor records of contract documents. Now, as each component attempts to reconcile obligations and verify services rendered and products delivered, different conclusions are being drawn. OBP, GSA, and the contractor are attempting to resolve the situation.

Recommendation 4: We recommend that the Commissioner, Customs and Border Protection, continue to work with GSA and the RVS contractor to settle remaining claims under the BPA, financially reconcile funding provided to GSA, and obtain the return of the unused funds to DHS.

Challenges Exist in Expanding Surveillance Coverage

Based on a review of RVS camera installation schedules and OBP records, these installations took, on average, 20 months to complete. The most time consuming aspect of installing RVS sites and associated infrastructure, involved site selection, securing land access, and performing environmental assessments. In some instances, these administrative activities took more than 12 months to accomplish. This requirement will continue to exist in completing future RVS camera sites, repeater tower sites, and supporting power infrastructure. An analysis of the process OBP used to install RVS sites identified possible causes for project delays. OBP used the following process:

1. OBP sector personnel identified potential RVS sites.

2. OBP headquarters personnel issued a scope of work to the contractor.

3. The contractor prepared a comprehensive technical and cost proposal to perform the work outlined in OBP's scope of work.

4. OBP reviewed the contractor's technical and cost proposal, worked with the contractor to resolve any issues and then request that GSA, via a TD, issue an award to the contractor to perform the work.

5. Under the BPA, the contractor validated the sites selected by OBP and conducted preliminary real estate coordination.[37]

6. After the contractor validated the sites selected by OBP and property access was secured, OBP tasked USACE, under a memorandum of agreement, to perform the environmental assessments before the

[37] Although, the RVS contractor was responsible for conducting preliminary real estate coordination, INS or CBP's leasing offices actually executed the lease documents.

contractor began the actual site installation.

7. If property access negotiations were unsuccessful or environmental restrictions existed, OBP would have to identify an alternate location to install desired ISIS equipment. This would require modifying the TD, and would potentially involve entering into subsequent lease agreement negotiations, and performing additional environmental assessments.

Much of this pre-construction activity was performed sequentially when some steps could have been performed concurrently. For example, USACE personnel could have been requested to perform informal consultation with state, tribal, and federal regulatory agencies and provided some preliminary assessment as to whether a potential negative environmental effect might exist as part of the site selection process, while other contract activities – such as preparing, reviewing, and approving the contractor's technical and cost proposals, validating selected sites, and preparing property access agreements – were being performed.

To meet the ambitious goals of ASI, a significant number of additional surveillance structures and supporting infrastructure will likely be required.[38] An analysis of linear miles of borderlands performed by Government Accountability Office (GAO) indicates that 75 percent of the northern border is either state or privately owned and 25 percent is federal or tribal land.[39] Along the southwest border, 57 percent is either state or privately owned, while 43 percent is federal or tribal land.

- Federal land encompasses national parks, national forests, wildlife refuges, and that regulated by the Bureau of Land Management. Some federal land is designated as wilderness area under the *Wilderness Act of 1964*, which generally prohibits the construction of permanent structures such as communication towers. Other federal land is designated as critical habitats for endangered and threatened species under the *Endangered Species Act*. Additionally, 36 federally recognized Indian tribes have land that is close, adjacent to, or straddles international boundaries with Mexico and Canada.

[38] According to OBP officials, the RVS system currently deployed provides approximately 5 percent border coverage given an average tower height of 70 feet and viewing range of 1.5 miles.
[39] GAO-04-590, Border Security: Agencies Need to Better Coordinate Their Strategies and Operations on Federal Lands (June 2004).

Table 3 - Ownership of Land Adjacent to the U.S. Northern and Southwest Borders

Land Owner	Miles Along the Northern Border	Miles Along the Southwest Border
State or Private	**2,980**	**1,080**
Federal and Tribal	**1,020**	**820**
Bureau of Indian Affairs	160	76
Bureau of Land Management	80	171
Fish and Wildlife Service	40	152
National Park Service	360	361
Forest Service	400	57

Source: GAO analysis of federal or tribal land by miles.

- Identifying and locating private landowners and negotiating leases and rights of entry agreements are time-consuming administrative activities. The lease itself may be costly depending on land values, especially in an area such as the Lake Erie shoreline.

Once land access is obtained, environmental assessments will need to be performed for all sites being considered for RVS camera, repeater tower, and supporting power infrastructure installations. Federal legislation such as NEPA requires that federal agencies analyze the proposed federal actions that could significantly affect the environmental quality, including a detailed analysis of alternatives to the proposed action. Depending on the level of environmental evaluation and coordination required, some of these activities could take months to complete.

Recommendation 5: We recommend that the Commissioner, Customs and Border Protection, develop strategies to streamline the site selection, site validation, and environmental assessment process to minimize delays of installing surveillance technology infrastructure.

If OBP is successful in obtaining land access and the subsequent environmental assessment is favorable, resistance to the installation of ISIS equipment from special interest groups, privacy advocacy groups, private landowners, tribal governments, and other concerned citizens may further complicate and delay the installation of camera sites or force OBP to pursue other alternate locations.

Given these factors, some sectors have been successful in getting permission from other governmental, as well as non-governmental sources, either to access video feeds from non-OBP cameras or to use non-OBP infrastructure to place RVS cameras. This strategy cannot be used in all locations where cameras are needed, but if access to property that meets strategic or tactical

objectives can be secured, this approach would accelerate the process of establishing surveillance coverage of the area.

Recommendation 6: We recommend that the Commissioner, Customs and Border Protection, expand the shared use of existing private and governmental structures to install remote surveillance technology infrastructure where possible.

Once installed, RVS camera sites cannot be easily moved to respond to changes in the traffic patterns of illegal aliens. During our field visits, we were provided a demonstration of "scope trucks," which are available in some sectors. While these vehicles do provide mobile camera surveillance, the video feed is only available to those in the vehicle and cannot be transmitted to a central location for central monitoring similar to equipment used by major news organizations that provide video feeds from remote locations.

With the acquisition of a UAV system, OBP mobile surveillance capability will increase OBP's ability to detect intrusion in those areas approved for UAV flight operations. Additionally, according to one senior OBP official, new technology is being tested which would integrate sensors and cameras with mobile ground and water surveillance radar systems. According to this OBP official, this technology will be further evaluated for deployment once the contractor that will serve as a prime integrator in addressing ASI requirements is selected.

Mobile surveillance technology will eliminate the need to lease property or perform costly and time-consuming environmental assessments. This technology would also allow OBP to move remote surveillance platforms to different locations in response to changing traffic patterns of illegal aliens.

Recommendation 7: We recommend that the Commissioner, Customs and Border Protection, continue to identify and deploy the use of non-permanent or mobile surveillance platforms that will increase OBP's ability and mobility to identify illegal border intrusions.

Management Comments and OIG Analysis

We issued our draft report on October 24, 2005, and met with CBP officials on November 2, 2005, to discuss the report. At that meeting, CBP provided additional technical comments for our consideration. Subsequently, we made changes to the draft report, as appropriate, and we issued a revised draft on November 14, 2005. Below is a summary of CBP's response to the report's recommendations and our analysis of their response. A copy of CBP's response, in its entirety, is recorded in Appendix B.

Recommendation 1: We recommend that the Commissioner, Customs and Border Protection, maximize integration opportunities and ensure that future remote surveillance technology investments and upgrades can be integrated.

CBP stated that the vision of the ASI surveillance system is to provide an integrated defense in-depth and that OBP is working to fully integrate border surveillance capabilities with ASI. CBP advised that the new technologies to integrate multiple sensory, monitoring, and information technologies will be procured after an ASI development and integration contractor has been selected, which is projected to be September 2006.

CBP's response did not indicate the specific actions it intends to take to resolve this recommendation or a reason for the nine-month lag before the award of the ASI development and integration contract. CBP indicated that work is progressing to fully integrate the border surveillance capabilities, however the exact nature of that work was not described. Further, the potential for contract award delays, and subsequent delays in implementing integration measures are viable threats to CBP meeting the intent of this recommendation. Therefore, we request that CBP describe the specific actions or activities to be accomplished or are planned before the ASI integration is realized.

Recommendation 1 – Unresolved - Open

Recommendation 2: We recommend that the Commissioner, Customs and Border Protection, standardize the process for collecting, cataloging, processing, and reporting ICAD intrusion and response data.

CBP stated that the recently released enhancements to the ICAD system provide aids and tools to improve and standardize the data collection process. CBP indicated that response data fields have been defined, which

should lead to more consistent recording of activity. The system can now accommodate latitude and longitude information, which will be useful in geospatial reporting. Additionally, recent ICAD enhancements make it easier for LECAs to associate cameras with sensor alarm tickets. However, CBP did not mention what steps it will take to standardize the data in the results fields. Currently, the data in the results fields are inconsistent across OBP sectors.

While CBP's actions are generally responsive to this recommendation, before we will close this recommendation, we request that CBP address how they intend to standardize usage of the results fields in ICAD.

Recommendation 2 – Resolved - Open

Recommendation 3: We recommend that the Commissioner, Customs and Border Protection, develop and apply performance measures that can evaluate whether current and future technology solutions are providing force-multiplication results and increasing response effectiveness in monitoring and detecting illegal intrusions along U.S. borders.

CBP stated they are applying performance measures that can evaluate the current technology in use by using the Border Patrol Enforcement Tracking System and the ICAD system. Additionally, CBP said that specific ASI requirements are based on established CBP operational requirements and are aligned with the DHS and CBP enterprise architecture.

Neither during our field visits nor in discussion with OBP headquarters personnel was the use of the Border Patrol Enforcement Tracking System mentioned as a method for measuring force multiplication benefits and response effectiveness. Therefore, we request that CBP further explain the Border Patrol Enforcement Tracking System, identify how long this system has been used to measure force multiplication benefits and response effectiveness, how this system, combined with ICAD system, is measuring force multiplication benefits and response effectiveness, and what is being measured.

Additionally, we request that CBP provide the referenced ASI requirements established for measuring force multiplication benefits and response effectiveness based on CBP's operational requirements.

Recommendation 3 – Unresolved - Open

Recommendation 4: We recommend that the Commissioner, Customs and Border Protection, continue to work with GSA and the RVS contractor to settle remaining claims under the BPA, financially reconcile funding provided to GSA, and obtain the return of the unused funds to DHS.

CBP's response outlined several significant steps, including regular meetings with GSA officials and representatives of the RVS contractor, it has taken to settle remaining claims under the BPA, reconcile funding provided to GSA, and recover the unused funds and return those funds to DHS. According to its response, CBP set a due date for these activities of November 30, 2006.

The actions CBP has taken thus far and the action they have identified to resolve this issue are responsive to this recommendation. When CBP provides evidence that the claims are settled and GSA accounts are reconciled, we will close this recommendation.

Recommendation 4 – Resolved – Open

Recommendation 5: We recommend that the Commissioner, Customs and Border Protection, develop strategies to streamline the site selection, site validation, and environmental assessment process to minimize delays of installing surveillance technology infrastructure.

CBP stated that it will implement strategies to streamline the site selection, site validation, and environmental assessment process through a Risk Management Plan, once the ASI prime integrator is selected. Additionally, CBP stated that the ASI Program Management Office has created a Risk Management Team and Risk Management Plan to manage risks, including overall streamlining of installing surveillance technology.

CBP's response did not indicate what specific actions it will take during the interim period before the ASI prime integrator is selected to mitigate delays in the site selection and validation, and the environmental assessment processes, or how the Risk Management Plan will streamline the installation of surveillance technology. We request that CBP specifically advise us of the actions or activities that will be taken to address this recommendation.

Recommendation 5 – Unresolved - Open

Recommendation 6: We recommend that the Commissioner, Customs and Border Protection, expand the shared use of existing private and governmental structures to install remote surveillance technology infrastructure where possible.

CBP advised that it will make every possible use of existing private and governmental structures to install future remote surveillance technology.

CBP did not indicate what specific actions it will take to identify desirable existing private and governmental structures for remote surveillance technology infrastructure installations or how it intends to negotiate the shared use of non-CBP structures. We request that CBP provide a description of the specific actions it will take to implement this recommendation.

Recommendation 6 – Unresolved – Open

Recommendation 7: We recommend that the Commissioner, Customs and Border Protection, continue to identify and deploy the use of non-permanent or mobile surveillance platforms that will increase OBP's ability and mobility to identify illegal border intrusions.

CBP stated that its goal is to use state-of-the-market technology, equipment, and infrastructure elements as new technologies are identified, and create a cost effective system that meets enforcement objectives at the lowest life cycle costs. CBP pointed out that it will incorporate a mix of both mobile and permanent surveillance technologies. Additionally, CBP listed several technologies that might be a part of ASI.

As the ASI contract is not expected to be awarded until September 2006, and the technologies listed are only potentially part of ASI requirements, we request that CBP provide a description of specific actions or activities that will be initiated prior to the proposed date when ASI non-permanent or mobile surveillance solutions are implemented.

Recommendation 7 – Unresolved – Open

Purpose, Scope, and Methodology

The purpose of our review was to determine the effectiveness of border surveillance, remote assessment, and monitoring technology in assisting CBP to detect illegal entry into the United States. In particular, we examined the capabilities, limitations, and support requirements of OBP's Integrated Surveillance Intelligence System equipment in monitoring activities along United States borders. Where ISIS equipment has been deployed, we assessed where additional ISIS coverage is needed as well as what is being done to address coverage deficiencies.

Additionally, we examined how CBP is measuring the effectiveness of these "force-multiplying" technologies to assess and respond to illegal traffic along northern and southwestern borders. Finally, we examined the process of how technology initiatives such as UAVs - which are under consideration for future use as part of the Arizona Border Control Initiative – are introduced, tested, and implemented. The focus of this review was on border surveillance along the United States Canadian and Mexican borders.

We collected and analyzed ISIS, ASI, and UAV information, provided by OBP. Also, we obtained and reviewed information from S&T regarding the technology development process. We interviewed officials from CBP-OIT and S&T Directorate in Washington, DC. Additionally, we received information from the GSA's Chicago regional office, which provided contract support to OBP for the installation of RVS equipment and ICAD systems, and the FAA, which provided information about the use of UAVs in the national airspace system.

We performed fieldwork between November 2004 and August 2005 at OBP headquarters in Washington, DC, and at OBP sector offices in Blaine, WA; Detroit, MI; Laredo, TX; Marfa, TX; Naco, AZ; Swanton, VT; and Tucson, AZ. We selected these border sectors based on (1) the amount and types of technology in the sector; (2) whether the sector had recently received either initial or additional technology equipment; and, (3) the general topography of the sector (only land, land and water, or mostly water). The three northern sectors selected are considered "focus" sectors by OBP for national security purposes.[40] Two of the selected southwest sectors were designated "focus" sectors.

[40] Some of the factors OBP uses to determine whether a sector is a "focus" sector includes the number of illegal alien apprehensions, the presence of well-organized smuggling organizations in the sector's areas of operation that are able to move large volumes of illegal aliens, and established infrastructure on both sides of the border that facilitates smuggling. This includes multiple avenues of ingress and egress from the border areas, and the existence of large U.S.

CBP officials recommended that we visit the Laredo and Blaine Sectors to observe the difference in video resolution between using microwave (wireless) and fiber optic (cable) transmissions. CBP officials also recommended that we visit Tucson Sector to observe UAV flight in support of OBP ground operations.

To evaluate the effectiveness of border surveillance, remote assessment, and monitoring technology, we sampled ICAD reports from three southwest border sectors (El Paso, Laredo, and Tucson) and three northern border sectors (Blaine, Grand Forks, and Swanton). For each sector, our sample included all tickets entered into the ICAD system throughout five 24-hour periods during April and May 2005, including tickets resulting from sensor alerts, RVS camera detections, and other non-ISIS sources, such as OBP agent, other agency, or citizen observations.

Finally, to assess the RVS camera procurement and installations process, we reviewed all applicable documentation for six of the 47 TDs issued under the BPA. Of those six, four directed RVS installations along the southwest border and two directed RVS installations along the northern border. Additionally, upon OBP's recommendation, we looked at one "worst case scenario" TD for work on the northern border that was issued under an earlier contract.

Our work was conducted under the authority of the *Inspector General Act of 1978*, as amended, and according to the *Quality Standards for Inspections* issued by the President's Council on Integrity and Efficiency.

metropolitan areas within driving distance of the border that are used as staging areas and that have transportation hubs to further the illegal entry into the United States.

U.S. Department of Homeland Security
Washington, DC 20229

U.S. Customs and Border Protection

Commissioner

December 5, 2005

MEMORANDUM FOR: RICHARD L. SKINNER
INSPECTOR GENERAL

FROM: Acting Commissioner Deborah J. Spero

SUBJECT: Response to the Office of Inspector General's Draft Report on Remote Surveillance Technology Along U.S. Land Borders

Thank you for providing us with a copy of your draft report entitled "A Review of Remote Surveillance Technology Along U.S. Land Borders" and the opportunity to discuss the issues in this report. As the report indicates, certain areas concerning future surveillance technology need to be addressed. U.S. Customs and Border Protection (CBP) acknowledges the existence of these problem areas and had already initiated solutions before issuance of the Office of Inspector General (OIG) report with the launching of the America's Shield Initiative (ASI). Identification of the issues highlighted in the report, along with the corrective measures being taken, will ensure that the proper border surveillance technology is used to detect illegal entry into the United States and to secure the homeland.

The OIG report provides valuable recommendations to be addressed with surveillance technology in border security. However, although CBP agrees with the seven recommendations, CBP does not concur with the overall content, tone, and balance of the report. The report contains inaccurate information and omits significant facts. The overall tone and balance of the report are negative towards the Office of Border Patrol (OBP). Many of the problems that the OIG identified in the report and attributed to OBP existed long before OBP took over managing the program in April 2001.

The report inaccurately states that OBP requested that the General Services Administration (GSA) issue a Blanket Purchasing Agreement (BPA) to International Microwave Corporation (IMC). This agreement was not entered into at the request of OBP. Before the creation of CBP in March 2003, the U.S. Border Patrol was part of the Department of Justice's U.S. Immigration and Naturalization Service (INS). Another office within the INS, the Office of Information Resources Management

(OIRM), requested and entered into a BPA between GSA and IMC in November 2000. Additionally, GSA served as the Contracting Officer (CO) and the Contracting Officer's Technical Representative (COTR) throughout the BPA.

In April 2001, the BPA was transferred to OBP through a Memorandum of Understanding signed by OIRM and OBP. When the BPA was transferred in 2001, OBP inherited a contract that had already been awarded by GSA and that included many problems. Because of the continuous unresolved prior and ongoing issues with the contract, OBP allowed the contract to lapse in September 2004, rather than renew it.

In regard to OBP oversight of contract activities, the OIG states in the report that there is limited evidence that OBP monitored contractor performance or fulfilled its responsibilities under the BPA to certify invoices. GSA was functioning and continued to function as CO and COTR when the contract was transferred to OBP. The report omits the significant fact that OBP questioned GSA regarding numerous invoices. OBP often did not receive any response from GSA to those inquiries, and the invoices were often paid by GSA without attempts to resolve the issues prior to payment. OBP was not the CO or the COTR and therefore had no control over the payment of invoices.

Comments that both GSA and OBP kept poor records are inaccurate. OBP was not the CO or COTR and did not award the contract; therefore, OBP would not have original records of the awarded contract or original invoices. But OBP does have approximately 90 percent of invoice copies. During the GSA OIG audit, GSA officials came to OBP requesting copies of the records in OBP's possession.

Additionally, because OBP was part of the INS and the Integrated Surveillance Intelligence System (ISIS) program was initiated while OBP was part of INS, an assumption is frequently made that OBP was responsible for the ISIS program from inception. However, OIRM was the program manager of the ISIS Program when the initial contract was awarded.

OBP has recognized the importance of the OIG recommendations and had made efforts to address them before issuance of the OIG report. OBP established ASI to provide an integrated surveillance system, including command and control capabilities, supporting Department of Homeland Security and CBP strategic goals and the Commissioner's priorities. ASI will provide the following:

- Permanent and mobile technology will be used.
- Electronic border surveillance capabilities will be fully integrated and expanded to all border areas based on threat.

- Tactical command and control will be enhanced and will establish situational awareness capabilities.
- Force-multiplying technologies will be expanded and decision support systems will be provided.
- Implementation will be streamlined and will be cost-effective.

CBP has established an ASI Program Management Office to oversee the use of technology, infrastructure, and staffing to secure U.S. borders. As part of the office's responsibility, it will ensure that a comprehensive acquisition strategy and contract administration plan are in place. CBP is committed to providing the tools and resources necessary to gain operational control of our Nation's borders.

Attached are comments specific to the recommendations. With regard to the classification of the draft report, CBP has not identified information within the report requiring restricted public access based on a designation of "For Official Use Only."

If you have any questions regarding this response, please contact me or have a member of your staff contact Ms. Lynn Richardson, Audit Liaison, Office of Policy and Planning, at (202) 344-2953.

Attachment

Response to Recommendations Concerning OIG Draft Report Entitled "A Review of Remote Surveillance Technology Along U.S. Land Borders"

U.S. Customs and Border Protection Corrective Action Plan

Recommendation 1: We recommend that the Commissioner, Customs and Border Protection, maximize integration opportunities and ensure that future remote surveillance technology investments and upgrades can be integrated.

Response: U.S. Customs and Border Protection (CBP) concurs with the recommendation. The Office of Border Patrol (OBP) has been delegated the authority and responsibility for border security and control between the ports of entry (POE). OBP established the ASI to provide surveillance and decision support technologies that will detect, characterize, and classify illegal breaches of the land border between the POE to assist Border Patrol agents in resolving incursions. The vision of the America's Shield Initiative (ASI) surveillance system is to provide an integrated defense in-depth that can support interdiction of internal and external threats operating in or moving through the land border between the POE.

OBP is working to fully integrate border surveillance capabilities with agent operations in all border areas with the ASI. Future technology will integrate multiple sensory, monitoring, and information technologies to provide timely data to decision makers at all levels of operations and administration. It will support maximum integration among all Department of Homeland Security (DHS) information system elements with regard to data and information sharing, deployment, and planning. Particularly significant are the interfaces with the Consolidated Enforcement Environment; external law enforcement systems, including the Federal Bureau of Investigation's criminal systems; and the new DHS U.S. Visitor and Immigrant Status Indicator system. There will also be interoperability between all pertinent local, state, and Federal law enforcement entities and other mission partners.

New technologies will be procured after the selection of the ASI development and integration contractor.

Due Date: The projected date for contract award is September 2006.

Recommendation 2: We recommend that the Commissioner, Customs and Border Protection, standardize the process for collecting, cataloging, processing, and reporting Intelligent Computer-Assisted Detection intrusion and response data.

Response: CBP concurs with the recommendation. During the week of November 7, 2005, OBP released the latest update of Intelligent Computer Assisted Detection (ICAD) III version enhancement. This update included the following:

> **Camera Association:** It will be easier to associate cameras with alarm ticket records. The new code filters the list of available cameras in the camera

combo box on the Alarm Tickets screen to match the station of the selected alarm ticket record.

Database Types: Database types will now be defined further into categories, which include Incident, Lead, or Procedure.

Geographical Data Table: ICAD will display up to six digits after the decimal point for longitude and latitude values.

Also incorporated are the following system change requests to improve cataloging and response data:

- The update standardized and defined response data fields.
- ICAD user account capacity was increased to 1,000 accounts per sector.
- ArcGIS 9 interface was added to allow geospatial reporting capability.

ICAD version III was released to all OBP sectors and their personnel.

Due Date: Completed November 7, 2005.

Recommendation 3: We recommend that the Commissioner, Customs and Border Protection, develop and apply performance measures that can evaluate whether current and future technology solutions are providing force-multiplication results and increasing response effectiveness in monitoring and detecting illegal intrusions along U.S. borders.

Response: CBP concurs with the recommendation. Specific ASI requirements are based on established CBP operational requirements and are in alignment with the DHS and CBP Enterprise Architecture. Contract performance will be managed through the application of Earned Value Management, the Contractor's CMMI Level 3 methodology, program management reviews, and design and milestone reviews. Once the contract is awarded to the development and integration Federal Acquisition Regulation contractor, the contract will also require metric system of measurement in accordance with 15 United States Code 205b (Federal Acquisition Regulation 11.002(b)) and DHS metrics plans and guidelines.

OBP is applying performance measures that can evaluate the current technology being used through the Border Patrol Enforcement Tracking System and the ICAD system for collecting, cataloging, and processing data. Selection of future technologies and software enhancements along with streamlined procedures will also provide the capability to measure, collect, and report network and sensor performance metrics.

Due Date: November 30, 2006

Recommendation 4: We recommend that the Commissioner, Customs and Border Protection, continue to work with the General Services Administration (GSA) and the RVS contractor to settle remaining claims under the Blanket Purchase Agreement, financially reconcile funding provided to GSA, and obtain the return of the unused funds to the Department of Homeland Security.

Response: CBP concurs with the recommendation. CBP continues to work closely with GSA and the contractor to finalize credits due back to the Government for incomplete installations and equipment. CBP sent a final list of recommendations to GSA on September 19, 2005, and is awaiting final documentation from GSA on credits due back to DHS.

CBP has been reviewing and commenting on invoices since November 2004. CBP participated in intermittent conference calls with GSA in the winter and early spring and met with L-3 on the invoices beginning in April 2005. Conference calls and meetings with L-3 and GSA were conducted several times in April, May, and June 2005. Additionally, meetings continued every Wednesday in June and July, including days spent at the L-3 facility on July 15, July 18, and August 3, 2005. Since GSA was given the final list of invoice recommendations, meetings have continued with GSA and L-3 on a weekly basis since the beginning of October. As of November 10, 2005, L-3 had sent several closeout files for review.

Due Date: November 30, 2006

Recommendation 5: We recommend that the Commissioner, Customs and Border Protection, develop strategies to streamline the site selection, site validation, and environmental assessment process to minimize delays of installing surveillance technology infrastructure.

Response: CBP concurs with the recommendation. Once the prime integrator is selected, strategies to streamline surveillance technologies, to include site selection, site validation, and the environmental assessment process, will also be implemented through the Risk Management Plan. The ASI Program Management Office has created a Risk Management Team and a Risk Management Plan that will document how risk management practices for the program will be instituted and implemented. Managing risks will produce benefits, such as early detection of problems, proactive solutions, improved use of resources, and overall streamlining of installing surveillance technology.

Due Date: November 30, 2006

Recommendation 6: We recommend that the Commissioner, Customs and Border Protection, expand the shared use of existing private and governmental structures to install remote surveillance technology infrastructure where possible.

Response: CBP concurs with the recommendation and will make every possible use of existing private and governmental structures to install future remote surveillance technology infrastructure where possible.

Due Date: November 30, 2006

Recommendation 7: We recommend that the Commissioner, Customs and Border Protection, continue to identify and deploy the use of non-permanent or mobile surveillance platforms that will increase the Office of Border Patrol's ability and mobility to remotely identify illegal border intrusions.

Response: CBP concurs with the recommendation. CBP's goal is to use state-of-the-market technology, equipment, software, and infrastructure elements as new technologies are identified, to create a cost-effective system that meets enforcement objectives at the lowest life cycle costs. CBP will incorporate a mix of both mobile and permanent surveillance technologies to identify illegal border intrusions. In addition, agents in the field will be provided the mobile capabilities to directly access and process data to identify illegal border intrusions. ASI system elements to be procured may include "intelligent" sensor and video technologies; mobile/portable information elements; mobile/portable sensor/video; decision support; command and control; multiuse agent devices (personal digital assistant, phone, Geographic Information System, sensor, and video); and aerial surveillance assets.

Due Date: November 30, 2006

Carlton Mann, Chief Inspector, Department of Homeland Security, Office of Inspections and Special Reviews

Moises Dugan, Senior Inspector, Department of Homeland Security, Office of Inspections and Special Reviews

Michael Zeitler, Inspector, Department of Homeland Security, Office of Inspections and Special Reviews

Jessica Barnes, Inspector, Department of Homeland Security, Office of Inspections and Special Reviews

Department of Homeland Security

Secretary
Deputy Secretary
Commissioner, Customs and Border Protection
Chief of Staff
Assistant Secretary for Public Affairs
Assistant Secretary for Legislative Affairs
General Counsel
Under Secretary, Science and Technology
Executive Secretary
Assistant Secretary for Policy
Chief Security Officer
DHS OIG Liaison

Office of Management and Budget

Chief, Homeland Security Branch
DHS Program Examiner

Congress

Congressional Oversight and Appropriations Committees, as appropriate

Additional Information and Copies

To obtain additional copies of this report, call the Office of Inspector General (OIG) at (202) 254-4100, fax your request to (202) 254-4285, or visit the OIG web site at www.dhs.gov.

OIG Hotline

To report alleged fraud, waste, abuse or mismanagement, or any other kind of criminal or noncriminal misconduct relative to department programs or operations, call the OIG Hotline at 1-800-323-8603; write to Department of Homeland Security, Washington, DC 20528, Attn: Office of Inspector General, Investigations Division – Hotline. The OIG seeks to protect the identity of each writer and caller.