STATEMENT OF

RICHARD L. SKINNER

INSPECTOR GENERAL

U.S. DEPARTMENT OF HOMELAND SECURITY

BEFORE THE

SUBCOMMITTEE ON MANAGEMENT, INTEGRATION, AND OVERSIGHT

COMMITTEE ON HOMELAND SECURITY

U.S. HOUSE OF REPRESENTATIVES

DECEMBER 16, 2005

Good morning Mr. Chairman and Members of the Subcommittee. Thank you for the opportunity to discuss the Office of Inspector General (OIG) review of the effectiveness of border surveillance, remote assessment, and monitoring technology in assisting the Department of Homeland Security's (DHS) Bureau of Customs and Border Protection (CBP) to detect illegal entry into the United States. [1]

Introduction

The Office of Border Patrol (OBP), within 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. To accomplish this mission, OBP uses a mix of agents, information, technology, and equipment.

The technology OBP uses includes cameras and sensors to detect and identify illegal border intrusions. OBP manages remote surveillance technology under the auspices of the Integrated Surveillance Intelligence System (ISIS) program and the America's Shield Initiative (ASI). Since Fiscal Year 1997, ISIS and ASI have received more than $429 million in funding. ISIS equipment includes sensors, the Remote Video Surveillance (RVS) system, and the Intelligent Computer Assisted Detection (ICAD) system. The key elements are as follows:

ISIS Equipment

- **Sensors**, primarily seismic and magnetic, buried in the ground, provide primary remote detection capability. When a sensor detects activity, alerts are sent via radio transmission to an OBP sector or station communications center. According to OBP, there are more than 11,000 sensors along the northern and southwest borders. Sensors are part of the first line of a layered border security strategy. Sensor technology is the most widely used as well as the easiest and least expensive to install and maintain.

- The **RVS system** provides the primary remote identification capability. The RVS system includes both color (day) and thermal-infrared (night) cameras, which are mounted on sixty or eighty-foot poles or other structures. The RVS system utilizes related infrastructure such as repeater towers, control room monitors, and toggling keyboards to zoom, pan, and tilt the cameras. As of August 2005, 255 RVS camera sites and 27 non-camera sites (repeater towers for example) are operational. There are 168 RVS camera sites and 38 non-camera sites that are incomplete.

- The **ICAD system** provides OBP with a resource tracking and response coordination capability. ICAD is integrated with the 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 Law Enforcement Communication Assistants (LECAs) in

[1] DHS OIG, *A Review of Remote Surveillance Technology along U.S. Land Borders* (OIG-06-15)

tracking OBP agent activities and provides OBP with a means to generate activity reports.

Law Enforcement Communications Assistants (LECA)

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 monitor both RVS camera and ICAD terminals. Once they observe suspicious activity or receive a sensor alert notification through ICAD, they relay the appropriate information to OBP agents who will investigate and report on the incident. When the results of the OBP agent's investigation are received, the LECA closes the ICAD ticket.

Results of Review

Several limitations of border surveillance, remote assessment and monitoring technology as well as significant delays and cost overruns in the procurement of the RVS system has impeded the success of ISIS.

ISIS Has Not Been Integrated

Since its introduction, ISIS has had varying expectations.[2] However, it is clear that sensors and RVS cameras were intended to work together, leveraging the detection capabilities of sensors with the visual identification capabilities of RVS cameras.

To date, ISIS components have not been integrated to the level predicted at the program's onset. RVS cameras and sensors are not linked whereby a sensor alert automatically activates a corresponding RVS camera to pan and tilt in the direction of the triggered sensor. However, 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.[3]

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 LECAs. The LECA is required to select the appropriate RVS camera, manually maneuver the camera in the direction of the sensor, and then attempt to identify the cause of the sensor alert.

[2] ISIS 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 ICAD component of ISIS with OIRM. In March 2003, when Border Patrol became a component of DHS, 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.

[3] According to OBP officials, the RVS system currently deployed provides approximately five percent border coverage given an average tower height of 70 feet and viewing range of 1.5 miles.

OBP Could Not Demonstrate Force-Multiplication Advantages of Technology

Senior CBP and OBP officials have made repeated statements in congressional testimony and program documents that ISIS is a force-multiplier. OBP officials asserted 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. However, OBP has not developed performance measures to evaluate the effectiveness of ISIS and its role as a force multiplier.

OBP officials pointed out that to measure accurately the force-multiplication benefits of ISIS technology requires an accounting of the number of attempted illegal entries and the number of attempts that were successful. 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, and because some OBP sectors are recording certain events in ICAD while other sectors are not, they also acknowledge that ICAD data would be of limited value and that conclusions drawn from this data would vary.

Several factors limit the accuracy of ICAD data, thereby limiting its usefulness for measuring force-multiplication benefits and response effectiveness. For example, LECAs may not always have time to advise an OBP agent of sensor alerts or camera observations. Similarly, OBP agents may not be available to respond. If there is a delay between the sensor alert or camera observation and when an OBP agent investigates the possible intrusion, the ticket may simply be cleared as "Unidentified," "Not Available," or "Unknown."

Few Apprehensions were Attributed to Sensor Alerts

Using sample ICAD data, we determined that more than 90 percent of the responses to sensor alerts resulted in "false alarms," something other than illegal alien activity, such as local traffic, outbound traffic, a train, or animals. On the southwest border, only two percent of sensor alerts resulted in apprehensions, and on the northern border, less than one percent of sensor alerts resulted in apprehensions.

Therefore, despite claims that ISIS prevents OBP agents from having to respond to false alarms, our analysis indicates that OBP agents are spending many hours investigating legitimate activities 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.

ISIS Procurement

Over the life of ISIS different contracts, regulations, and agreements have affected the installation of the RVS sites, including, Federal Acquisition Regulations, General Services Administration (GSA) federal supply schedule contracts with various vendors, particularly the federal supply schedule contracts with International Microwave Corporation (IMC), and a Blanket Purchase Agreement (BPA).

In September 1998, the INS entered into an interagency agreement with GSA through a Memorandum of Understanding (MOU). 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, IMC was awarded a contract to engineer, install, manage, and provide remote surveillance equipment and support to multiple sites throughout the United States.

Following the initial award to IMC, INS requested that GSA issue a BPA to IMC. INS cited cost savings as the greatest benefit of a BPA. Specifically, INS highlighted a unique teaming alliance that 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, INS 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 to IMC for an estimated $200 million in purchases to support all RVS requirements through September 30, 2004. Only ISIS technology and OBP agent support equipment and services could be ordered under this BPA.

OBP's Oversight of RVS Equipment Contract Activities was Ineffective

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.

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

In addition, completed work was not finished in a timely manner, and more than $37 million in DHS funds remain unspent in GSA accounts.

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 invoices and certifications to GSA for payment.

Currently, OBP is certifying invoices after the invoices have been paid. OBP 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. PMC did recommend rejection of a few invoices. Most invoices were neither accepted nor rejected by OBP. In the six TDs in our sample, only seven invoices were recommended for payment in the certification emails, although according to GSA records, 65 invoices submitted by the contractor for these six TDs were paid in full. No invoices were rejected. However, the certification emails did include rejections of a few invoices for TDs that were not in our sample.

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

OBP Made Some Efforts to Bring the Contractor into Compliance with the BPA

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 regarding the contractor's performance. 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, GSA continued to pay invoices that the contractor submitted after this letter was sent. 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.

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.

Much of this pre-construction activity was performed sequentially when some steps could have been performed concurrently. For example, U.S. Army Corps of Engineers personnel could have performed informal consultation with state, tribal, and federal regulatory agencies and provided a preliminary assessment as to whether a potential environmental consideration 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 in progress.

To meet the ambitious goals of ASI, a significant number of additional surveillance structures and supporting infrastructure will likely be required. 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 the National Environmental Policy Act 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.

If OBP successfully obtains land access and favorable subsequent environmental assessments, 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 or delay the installation of camera sites or force OBP to pursue alternate locations.

Some sectors have been successful in getting permission from other governmental, as well as non-governmental sources, to either access video feeds from non-OBP cameras or to install RVS cameras on non-OBP infrastructure. 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.

Another limitation to current surveillance coverage is that once installed, RVS camera sites cannot be easily moved to respond to changes in the traffic patterns of illegal aliens. During our field visits, OBP demonstrated mobile surveillance technology or "scope trucks," which are available in some sectors. Mobile surveillance technology will eliminate the need to lease property or perform costly and time-consuming environmental

assessments. Also, this technology could allow OBP to move remote surveillance platforms to different locations in response to changing traffic patterns of illegal aliens.

Unmanned Aerial Vehicles for Border Security

OBP's use of Unmanned Aerial Vehicles (UAVs) along a portion of the southwest border is one positive step toward using mobile technology. Nevertheless, challenges remain in expanding the use of UAVs, as well. 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.

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.

Recommendations

We recommended 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.

In its response, CBP concurred with all seven of our recommendations. However, we regarded five of their responses insufficient to resolve our recommendations, and we have requested that CBP provide additional information in those instances.

Additionally, six of CBP's responses to our recommendations mention ASI. ASI is being subsumed into the much broader Secure Border Initiative (SBI). As a result, ASI has been put on hold according to OBP. In CBP's response, they indicate that a key milestone toward ASI implementation will be the selection of a development and integration contractor, which is projected occur in September 2006. Given the uncertainty of when, or if, ASI implementation as currently envisioned by CBP, we asked CBP to provide specific actions or activities that it will take prior to the proposed implementation date of ASI to resolve our recommendations.

Mr. Chairman, this concludes my prepared statement. I will be pleased to answer any questions you or the members may have.

# # #